SKDAV GOVT. POLYTECHNIC ROURKELA

E - COMMERCE

PREPARED BY
BIJAYALAXMI PADHIARY
SKDAV GOVT. POLYTECHNIC, ROURKELA

CHAPTER - 1
INTRODUCTION TO E-COMMERCE

1.1Introduction

Commerce is the exchange of something of value‖ between two entities. That something‖ may be goods, services, information, money or anything else the two entities consider to have value. As we enter the electronic age the question arises whether these business activities could be carried out electronically.

1.2What is E-commerce

- It is buying and selling of products and services by businesses and consumers through an electronic medium, without using any paper documents.
- Different application areas of e-commerce are
  - ❖Education
  - ❖Banking
  - ❖Online order processing
  - ❖Telecommunication
  - ❖Financial services like stocks
  - ❖Manufacturing
  - ❖Entertainment
  - ❖Customer relationship management
- E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce.
- It includes all inter-company and intra-company function (such as marketing, finance, manufacturing, selling, and negotiation) that enable commerce and use electronic mail, EDI, file transfer, fax, video conferencing, workflow, or interaction with a remote computer.

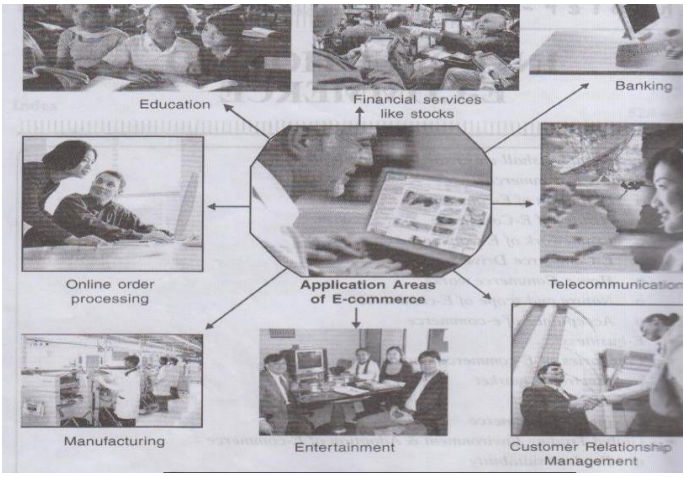


Fig 1.1 Different application areas of e-commerce

E-commerce can be defined from various perspective

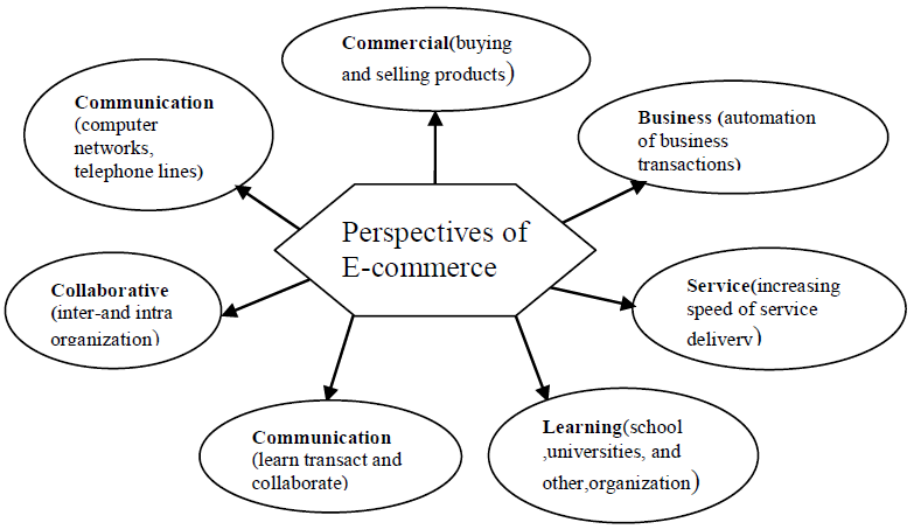


Fig.1.2 Different perspective of e-commerce

- **Communication perspective:**
  From a communication perspective, e-commerce is the delivery of good, service, information or payment over computer network, telephone lines or any other electronics means.
- **Business perspective**:
  From a business perspective, e-commerce is the application of technology toward the automation of business transactions.
- **Service perspective**:
  From service perspective, e-commerce is a tool that addresses the desire of firms, consumers and management to cut service cost while improving the quality of goods and increasing speed of service delivery.
- **Commercial(**trading**) perspective**:
  From a commercial perspective, e-commerce provides the capability of buying and selling product, services and information on the internet and via other online services.
- **Learning perspective**:
  From a learning perspective, e-commerce is an enabler of online training and education in schools, universities, and other organizations.
- **Collaborative perspective**:
  From a collaborative perspective, e-commerce is the frame work of inter-and-intra organizational collaboration.
- **Community perspective**:
  From a community perspective, e-commerce provides a gathering place for community members to learn transect and collaborate.

Framework of E-Commerce

Framework tells about the detail of how e-commerce can take place. It defines actually how e-commerce is implemented, how online trading or business can be done. It defines important components that should be present to do some transaction. The Framework of E-Commerce shown in the fig.1.2.

- The EC applications are supported by infrastructures.
- Their implementation is dependent on four major areas such as people, public policy, technical standards & protocols & other organizations.
- The EC management coordinates the applications, infrastructures, & pillars. It also includes internet marketing & advertisement.

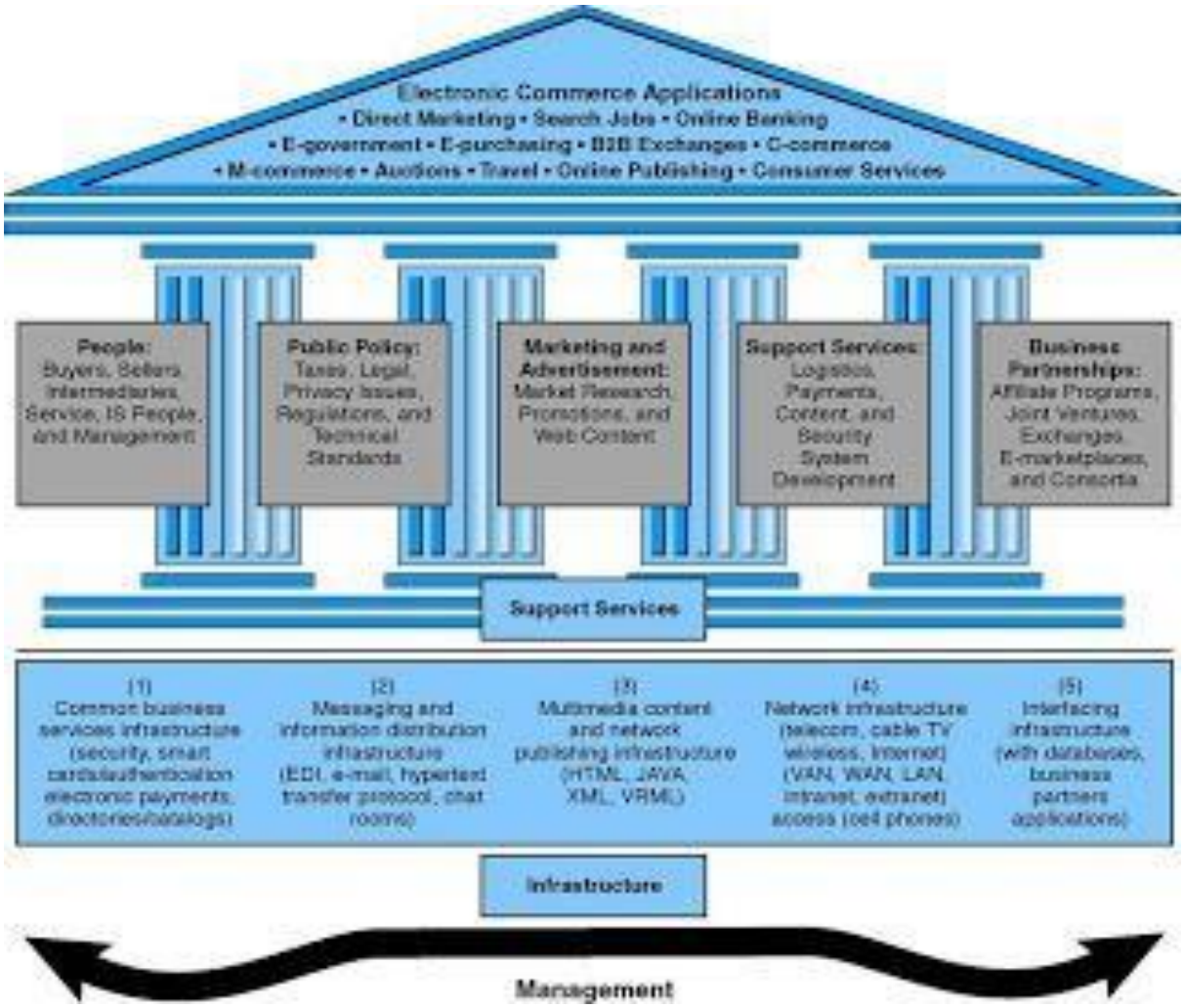


Fig.1.3. Framework of e-commerce

E-Commerce Drivers:

There are six drivers that promote E-Commerce as shown in Fig.1.3.

- ❖ Digital convergence:

Digital devices can now communicate with one another. The Internet made it all possible.

- Anytime, anywhere, anyone (Ubiquity):

  This means that anyone can communicate with the e-merchant or shop online 24 hours a day from anywhere in the world.

- Changes in organizations:

  Knowledge workers at the lower level in the organization can now take on responsibilities were once were relegated to lower or junior managers. The focus is on empowerment.

- Information Density:

  Global competitions and the proliferation of products and services worldwide have added unusual pressure to keep a close watch on operating costs and maximize profit margin. E-Commerce addresses these concerns quickly (efficiently), effectively and at low cost.

- Personalization/Customization:

  Today‘s customers are expecting higher quality and better performance, including a customized way of producing delivering and paying for goods and services. Mass customization puts pressure on firms to handle customized request on a mass market scale.

History of E-Commerce

- In 1970s e-commerce meant the facilitation of commercial transactions electronically, using technology such as electronic data interchange (EDI) & electronic funds transfer (EFT), allowing businesses to send commercial documents like purchase orders or invoices electronically.
- In 1980s e-commerce meant the facilitation of commercial transactions electronically, using technology such as the growth and acceptance of credit cards, automated teller machines (ATM), telephone banking, and airline reservation system help the businesses.
- In 1990s the internet commercialized and users flocked to participate in the form of dot-coms, or internet start-ups & innovative applications ranging from online direct sales to e-learning experiences.
- In 2000s many European &American business companies offered their services through the World Wide Web. Since then people began to associate a word ―E-Commerce‖.

How E-Commerce works:

The consumer moves through the internet the merchant‘s web site. From there he decides that he wants to purchase something. So he is move to the online transaction server where all of the information he gives is encrypted. Once he has placed his order, the information moves through a private gateway to a processing network, where the issuing and acquiring banks complete on deny the transaction. This generally takes place in no. more than 5-7 seconds. There are many different payment systems available to accommodate the varied processing needs of merchants from those who have a few orders a day to those who process thousands of transactions daily. With the addition of secure Socket Layer technology

eCommerce is also a very safe way to complete transaction. How E- Commerce works shown in the fig.1.4.

Fig.1.4. Working of E-Commerce

Nature & Scope of E-Commerce

Nature of E-Commerce

E-Commerce is a modern business methodology, which helps the companies and the consumers to have better business facilities through less cost while improving the quality of goods and services and increasing the speed of transaction.

E-Commerce covers online selling and transaction, web retailing and wholesaling, electronic data and fund transfer, electronic banking interactive marketing etc. It involves multimedia, advertising, product information, and customer support on the World Wide Web via internet, payment mechanism through bank etc.

Scope of E-Commerce

The scope of e-commerce is very wide. It connected the management of the enterprises to the various aspects of trading viz, suppliers, distrusters, retailers, consumers and well other trades on the global e-commerce infrastructure. The enterprises provide products development, conferencing, accounting, financial planning, and logistics etc. through e-commerce. The E- Commerce workflow diagram shows the various scope of E- commerce in fig.1.5.

- With suppliers it mainly concerns product sourcing, information; purchase process, supplier‘s management etc.
- With distributors and retailers it involves market response, inventory, product information, order fulfillment, accounts etc.
- With consumers it is mainly web marketing, e-shopping, information & online services, trading, service and sales etc.

  On the global e-commerce infrastructure, it mainly is about security, e banking, legal issues, e-market information, human-computer interface, national/global information infrastructure.

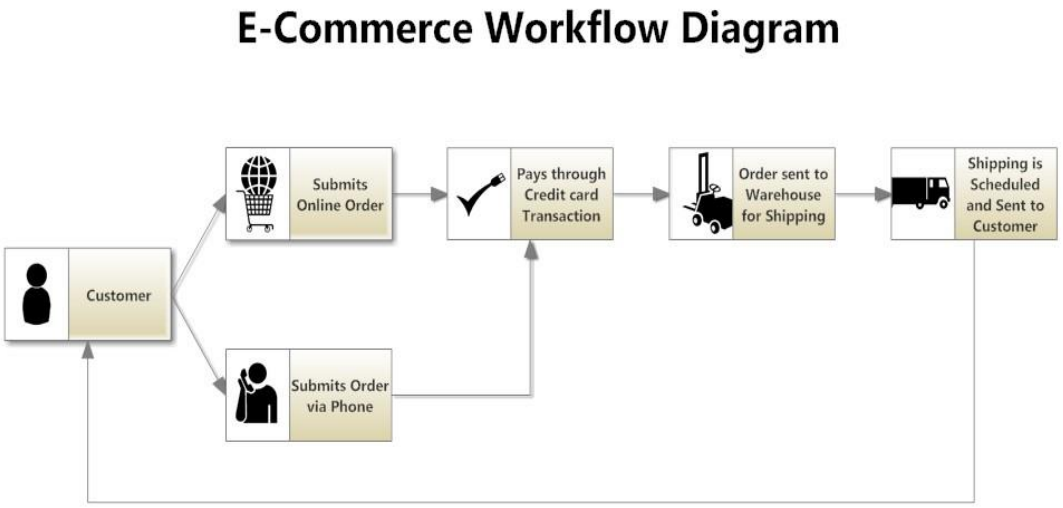


Fig.1.5. Scope of E-Commerce

1.3E-Business

E-Business or Electronic Business is the administration of conducting business via theInternet. This would include the buying and selling of goods and services, along with providing technical orcustomersupportthrough the Internet. E-Business is a term often used in conjunction withe-commerce, but includes services in addition to the sale of goods.

❖ **Difference between E-business & E-commerce**

- E-business is broader in scope and e-commerce is just an aspect or a subset of it. E-
- business refers to all online business transactions including buying and selling directly to consumers (e-commerce), dealing with manufacturers and suppliers, and conducting interactions with partners. Business functions are only limited to the companies' technological resources.
- E-commerce essentially involves monetary trade while in e-business, money transactions are not necessary.
- E-business involves marketing, product design, consumer service evaluation, and more.

E-business is frequently used interchangeably with E-Commerce.

1.4 Categories of E-Commerce Application

E-Commerce systems include commercial transactions on the internet but their scope is much wider than this. They can be classified by application type as:

- E-Markets
- EDI
- Internet Commerce

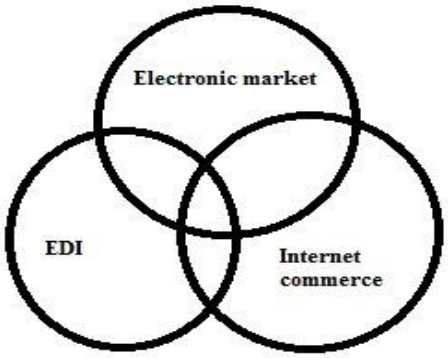


Fig 1.6. Categories of E-Commerce application

E-Markets:

The principle function of an electronic market is to facilitate the search for required product or services. Airline booking systems are an example of an electronic market.

Electronic data interchange :-

Electronic data interchange (**EDI**) is an electronic communication method that provides standards for exchanging data via any electronic means. By adhering to the same standard, two different companies, even in two different countries, can electronically exchange documents (such as purchase orders, invoices, shipping notices, and many others).

Internet commerce:-

The internet (and similar network facilities) can be used for advertising goods and services and transacting one-off deals. Internet commerce helps application for both business – to-business and business to consumer transactions.

1.5 Global trading environment & adoption of ecommerce

E-commerce has given a global platform to the manufacturers, traders, sellers & buyers or consumers. Now seller can treat world as a global market and buyers also have a wide range of choice to buy any product from anywhere in the world.

Some of possible factors to make it successful are

- Providing value to customers.

Venders can achieve this by offering a product or product –line that attracts potential customers at a competitive price, as in non-ecommerce.

- Providing service & performance.

  Offering a responsive, user-friendly purchasing experience, may go some way to achieving these goals.

- Providing an attractive website.

  The tasteful use of color, graphics, animation, photographs, fonts, and white-space percentage may aid success in this respect.

- Providing an incentive for customers to buy and to return.

  Sales promotions to this end can involve coupons, special offers, and discounts. cross-linked websites and advertising affiliate programs can also help.

- Providing personal attention.

  Personalized web sites, purchase suggestions, and personalized special offers may go some of the way to substituting for the face-to-face human interaction found at a traditional point of sale.

- Providing a sense of community.

  Chat rooms, discussion boards, soliciting customer input, loyalty schemes & affinity programs can help.

- Providing reliability & security

  Parallel servers, hardware redundancy, fail-safe technology, information encryption, & firewalls can enhance this requirement

- Providing a 360 degree view of the customer relationship, defined as ensuring that all employees, suppliers, & partners have a complete view, & same view of the customer.
- Owning the customer‘s total experience.

  E-tailers foster this by treating any contacts with a customer as part of a total experience, an experience that becomes synonymous with the brand.

- Streamlining business processes, possibly through re-engineering and information technologies.
- Letting customers help themselves.

  Provision of a self-serve site, easy to use without assistance, can help in this respect.

- Helping customers do their job of consuming.

  E-tailers can provide such help through ample comparative information and good search facilities .Provision of component information and safety – and –health comments may assist e-tailers to define the customer‘s job.

- Engineering an electronic value chain in which one focuses on a ―limited‖ number of core competencies – the opposite of a one-stop shop.
- Operating on or near the cutting edge of technology and staying there as technology changes (but remembering that the fundamentals of commerce remain indifferent to technology.)

- Setting up an organization of sufficient alertness and agility to respond quickly to any changes in the economic, social and physical environment.
- Product suitability : Certain product s/services appear more suitable for online sales; others remain more suitable for offline sales .Many successful purely virtual companies deal with digital products, including information storage, retrieval ,and modification, music, movies, education, communication, software ,photography, and financial transactions. Example of this type of company includes Google, eBay, Schwab, Morpheus etc.

1.6 Comparison between Traditional and E-Commerce

- Direct interaction is present in traditional commerce.
- E-commerce proves to be feasible for the standard products, low-value products , intangible products and digital products.
- In traditional commerce customer can verify the identity of the seller and their physical location, whereas in e-commerce customers feel insecure because they cannot identify the seller and are unaware about many things
- Traditional commerce is the best when it comes to convincing the customers on certain products.
- E-commerce uses e-cash, credit cards , debit cards and etc,.
- E-commerce is developing a highway system called the information super highway as we have the interstate highway system for traditional e-commerce.

1.7 Advantages & Disadvantages of E-Commerce

Advantages

1. Cost Effective

The entire financial transactions will eventually become electronic, so sooner conversion is going to be lower on cost. It makes every transaction through e-commerce payment a lot cheaper.

2. Higher Margin

E-commerce also enables us to move better with higher margin for more business safety. Higher margin also means business with more control as well as flexibility. You can also save time from the e-commerce.

3. Better Productivity

Productivity here means productivity for both companies and customers. People like to find answers online because it is faster and cheaper, and it costs a lot cheaper expense as well for the company.

4. Quick Comparison

E-commerce also enables you to compare price among several providers. In the end, it leads you to smart shopping. People can save more money while they shop.

5. Economy Benefit

E-commerce allows us to make transaction without any needs on stores, infrastructure investment, and other common things we find. Companies only need well built website and customer service.

Acceptance of E-Commerce

Consumers have accepted the e-commerce business model less readily than its proponent originally expected. Even in product categories suitable for ecommerce, e-shopping has developed only slowly. Several regions might account for the slow uptake including:

- Concern about security. Many people will not use credit cards over Internet due to concerns about theft and fraud.
- Lack of instant gratification with most e-purchases (non-digital purchases). Much of a consumer‘s reward for purchasing a product lies in the instant gratification of using and displaying that product. This reward does not exist when one‘s purchases do not arrive for days or weeks.
- The problem of access to web commerce, particularly for poor household and for developing countries. Low penetration rates of Internets access in some sectors greatly reduces the potential for e-commerce.
- The social aspect of shopping. Some people enjoy talking to sales staff, to other shoppers, or to their cohorts: this social reward side of retail therapy does not exist to the same extent in online shopping. **So the major disadvantages can be outlined as:**

Disadvantages

1.Security

Customers need to be confident and trust the provider of payment method. Sometimes, we can be tricked. Examine on integrity and reputation of the web stores before you decide to buy.

2. Scalability of System

A company definitely needs a well developed website to support numbers of customers at a time. If your web destination is not well enough, you better forget it.

3. Integrity on Data and System

Customers need secure access all the time. In addition to it, protection to data is also essential. Unless the transaction can provide it, we should refuse for e-commerce.

4. Products People

People who prefer and focus on product will not buy online. They will want to feel, try, and sit on their new couch and bed.

5. Customer Service and Relation Problem

They sometimes forget how essential to build loyal relationship with customers. Without loyalty from customers, they will not survive the business.

CHAPTER - 2
BUSINESS MODELS OF E-COMMERCE

2.1 Introduction

E-Business involves changes in an organizations business & functional processes with the application of technologies of the new digital economy. It is an internet initiative which transforms business relationships. It includes all aspect of ecommerce.

2.2 Business Models of E-Commerce

Creating an e-commerce solution mainly involves creating and deploying an ecommerce site. The first step in the development of an e-commerce site is to identify the e-commerce model. Depending on the parties involved in the transaction, ecommerce can be classified into 5 models. These are:

- Business – to – Consumer (B2C) model
- Business – to – Business (B2B) model
- Consumer – to- Consumer (C2C) model
- Consumer – to – Business (C2B) model
- Business – to – Government (B2G) model

2.3 Business-to-Consumer (B2C) Model

The B2C model involves transactions between business organizations and consumers. It applies to any business organization that sells its products or services to consumers over the Internet. These sites display product information in an online catalog and store it in a database. The B2C model also includes services online banking, travel services, and health information. The B2C model displays in fig.2.1.

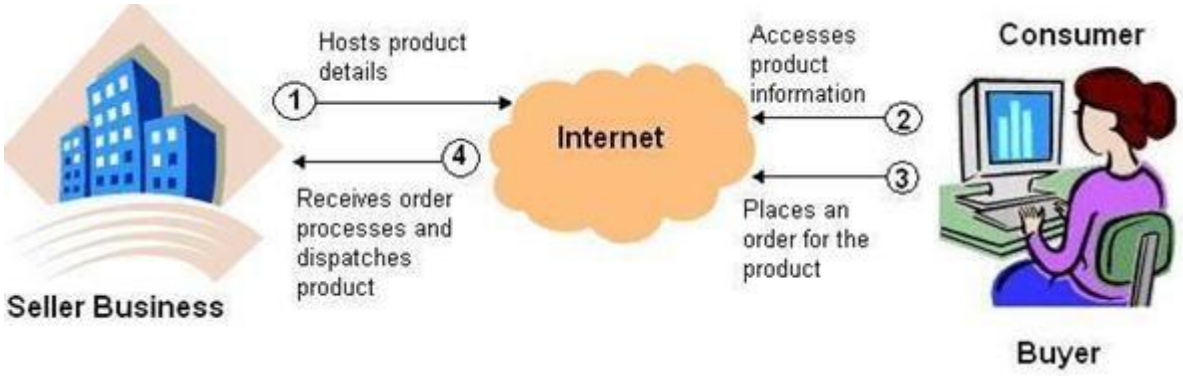


Fig.2.1. B2C Business model

Major activities of B2C E-Commerce

There are five major activities involved in conducting B2C e-commerce. The B2B ecommerce model uses a similar cycle, as shown in fig.2.2.

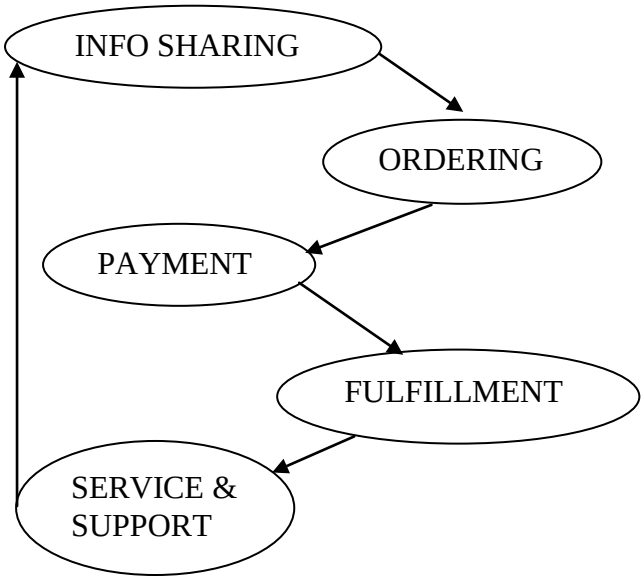


Fig.2.2. Major Activities for B2C e-commerce.

1. **Information sharing:**

   A B2C e-commerce may use some or all of the following applications and technologies to share information with customers: Online advertisements, e-mail, newsgroups/discussion groups, company web site, online catalogs, message board systems, bulletin board systems, multiparty conferencing.

2. **Ordering**:

   A customer may use electronic e-mail or forms available on the company's web site to order a product from a B2C site. A mouse click sends the essential information relating to the requested piece(s) to the B2C site.

3. **Payment:**

   Credit cards, electronic checks, and digital cash are among the popular options that the customer has as options for paying for the goods or services.

4. **Fulfillment:**

Fulfillment that is responsible for physically delivering the product or service from the merchant to the customer. In case of physical products(books, videos, CDs), the filled order can be sent to the customer using regular mail, MNG, Yurtiçi Cargo, FedEx, or UPS. As expected for faster delivery, the customer has to pay additional money. In case of digital products (software, music, electronic documents), the ebusiness uses digital documentations to assure security, integrity, and privacy of the product. It may also include delivery address verification and digital warehousing that stores digital products on a computer until they are delivered. The e-business can handle its own fulfillment operations or outsource this function to third parties with moderate costs.

5. **Service and support:**

It is much cheaper to maintain current customers than to attract new customers. For this reason, e-businesses should do whatever that they can in order to provide timely, high-quality service and support to their customers. As e-commerce companies lack a traditional physical presence and need other ways to maintain current customers, service and support are even more important in e-commerce than traditional businesses. The following are some examples of technologies and applications used for providing service and support: (E-mail confirmation, periodic news flash, and online surveys may also be used as marketing tools.) ❖<u>E-mail confirmation</u>:

In most cases, the e-mail confirmation provides the customer with a confirmation number that the customer can use to trace the product or service. E-mail confirmation promises the customer that a particular order has been processed and that the customer should receive the product/ service by a certain date.

- <u>Periodic news flash</u>:

  They used to give customers with the latest information on the company or on a particular product or offering.

- <u>Online Surveys</u>:

  Their results can assist the e-commerce site to provide better services and support to its customers based on what has been collected in the survey, even though online surveys are mostly used as a marketing tool.

- <u>Help desks:</u>

  They provide answers to common problems or provide advice for using products or services. They are used for the same purpose as in traditional businesses.

- <u>Assured secure transactions & assured online auctions:</u>

  They guarantee customers that the e-commerce site covers all the security and privacy issues. As many customers still do not feel comfortable conducting online business, the security and privacy services are especially important.

Model of B2C

B2C identified various kinds of models which are:

- Auction
- Online stores
- Online services

Auctions:

Electronic actions (on the Internet) offer electronic implementations of bidding mechanism also known from traditional auctions. This can be accompanied by multimedia presentation of the goods. Usually they are not restricted to this single function. They may also offer integration of the bidding process with contracting, payments and delivery. The sources of income for the action provider are in selling the technology platform, in transaction and collection of e-shops that gets usually enhanced by a common umbrella, for example of a well-known brand. It might be enriched by a common guaranteed payment method.‖

Advantages of Internet auctions:

Convenience:

It gives the participants convenience, as bidder can stay at his home or office and still participate in the bidding just as in traditional actions. It is also more convenient for a bidder to find more about the goods being auctioned.

Flexibility:

Traditional auctions allow only synchronous bidding requiring all bidders to participate at the same time. In contrast, Internet auctions allow asynchronous bidding lasting days or weeks, which offers more flexibility to the bidders.

Increased reach:

The potential of reach of an Internet based auction site is global and thus the market for auctioned good is very large.

Economical to operate:

These are cheaper to run as lot of costs relating to infrastructure required for a conventional auction system is not necessary for this.

Dis-advantages of Internet auctions

Inspection of goods:

In an internet based auction, it is not possible to physically inspect the goods. The bidders have to rely on the information provided or sometimes, may have to rely on the information provided or sometimes, may have to rely on some electronic images of the goods on auction.

Potential for fraud:

Internet bidder has to trust that the seller would actually send the good for which he paid. Also the payments are made by providing credit card details through the internet, which may always safe.

Online Stores:

Online stores refer to marketing of a company's product through the web. It may be done either to promote the company & its products & services or to actually sell the products/services through this virtual store. Amazon.com is one of the best examples of an estore which started selling books online & gradually extended to other product categories.

Benefits for the company

- Increased demand
- A low cost route to global reach
- Cost-reduction of promotion and sales
- Reduced costs

Benefits for the customers

- Lower price
- Wider choice
- Better information
- Convenience

Shopping through the online stores is fast gaining popularity & acceptance. Although majority of the revenue is in the B2B sales, B2C sales are also expected to improve in the coming years. However for this to occur, online stores need to deliver far more value to the customers & at the same times find new ways to generate revenues.

Delivering value to customers

- Merchants have to try to find ways to gain competitive advantage in factors other than just the price.
- Online shops need to provide a shopping-experience that addresses all of the customer's requirements. It should also try to provide an environment that is easy to explore.
- Expansion of the range of services.
- Find cost effective ways to increase customer base & generate higher revenues.

Online Services:

Many companies are using internet to provide customer service. Service sector banking & stock trading is one of such example. Companies like Markethemove.com & eTrade.com have brought the ease of trading stocks to customer's PC.

Types of B2C

B2C companies divide into five major categories: direct sellers, online intermediaries, advertising-based models, community-based models and fee-based models. Each type is so different from the others that they are not directly comparable. In fact, some B2C businesses utilize more than one type to reach different audiences.

➢**Direct Sellers**

Direct sellers, such as online retailers, sell a product or service directly to the customer via a website. Direct sellers can divide into e-tailers and manufacturers. E-tailers are electronic retailers that either ship products from their own warehouses or trigger deliveries from other companies & stocks. Product manufacturers use the Internet as a catalog and sales channel to eliminate intermediaries.

➢**Online Intermediaries**

Online intermediaries perform the same function as any other broker. The business allows non-B2C companies to reap some of the benefits. Brokers offer buyers a service and help sellers by altering the price-setting processes, according to economics professors.

➢**Advertising-Based Models**

Popular websites rely on advertising-based models. These websites offer a free service to consumers and use advertising revenue to cover costs. They draw a large number of visitors, making them ideal advertising streams for other companies. Advertisers will pay a premium to sites that deliver high traffic numbers.

➢**Community-Based Models**

Community-based models combine the advertising method that relies on traffic at sites that focus on specialized groups to create communities. Community sales and advertising take advantage of social and network marketing by focusing on specific groups that want specific products. For example, sites used by computer programmers are perfectly placed to advertise computer hardware and software products. At least one social media website uses member information to target advertisements to interests and locations.

➢**Fee-Based Models**

Pay-as-you-buy or paid subscription services fall under fee-based models. The most common of these are online subscriptions to journals or movie sites such as NetFlix. These companies rely on the quality of their content to convince consumers to pay a usually nominal fee.

<u>Major challenges of B2C E-Commerce</u>

❖ **Getting browsers to buy things:**

Getting visitors to the site is only half the battle. Customers are still abandoning their online shopping carts for a number of reasons, including clunky design. HTML is the cause of the most of the usability problems associated with ecommerce. Now broadband is more widespread, companies are boosting their conversion rates by deploying more advance web technologies & rich media. Some technologies include: flash application s, audio & video, ―bots‖ or s/w agents & real time analytics, Ajax (Asynchronous JavaScript & xml) are helping companies build more interactive websites.

❖ **Building customers trust/privacy:**

Companies need to take steps to ensure their customer information is well protected. Companies should secure web transaction using the secure socket layer protocol. They should also consider two part authentication, which can combine passwords with a security key with a changing code.

❖ **Building customer loyalty:**

Customer loyalty is particularly important given the fact that more consumers are using search engines to research product online, rather than going directly a particular store‘s site , how can you build a strong relationship with customers. Hera some tips

. Focus on personalization: A wide array of software is available to help ecommerce sites create unique boutiques that target specific customers.

- Create an easy – to –use customer service application .Providing just an e-mail address can be frustrating to customer with questions. Live chat or, at the very least, a phone number will help.
- Focus on making your site easy to use.

❖ **Fulfillment:**

E-commerce has increased the focus on customer satisfaction and delivery fulfillment, when fulfillment problems caused some Christmas order to be delivered late, then companies have spent billions to improve their logical system in order to guarantee on time delivery.

Advantages of B2C E-Commerce:

- ❖ Shopping can be faster and more convenient.
- ❖ Offerings and prices can change instantaneously.
- ❖ Call centers can be integrated with the website.
- ❖ Broadband telecommunications will enhance the buying experience.

2.4 Business-to- Business (B2B) Model

The B2B model involves electronic transactions for ordering, purchasing, as well as other administrative tasks between houses. It includes trading goods, such as business subscriptions, professional services, manufacturing, and wholesale dealings. Sometimes in the B2B model, business may exist between virtual companies, neither of which may have any physical existence. In such cases, business is conducted only through the Internet.The B2b Business model is shown in fig.2.3.

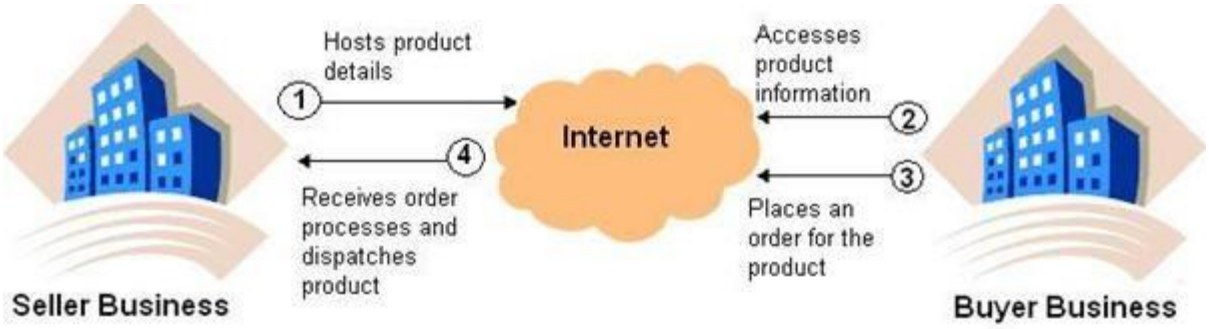


Fig.2.3. B2B Business Model

Activity of B2B E-Commerce

- B2B activity refers to all e-commerce transaction s that can occur between two organizations. This includes purchasing & procurement, supplier management, inventory management, channel management, sales activities, payment management & service & support.
- B2B include online companies that specialize in marketing strategies, advertising, email companies, internet consultants, website development etc.
- It is that portion of the internet market where transactions between organizations and their partners take place. It involves information about development, manufacturing, delivery, sales etc of product and services.
- A well –executed B2B system can take care of a wide spectrum of activities .It can take up the roll of a number of workers of a company. It reduces the cycle time substantially. It assists a firm in replacing the existing business practices with new, quick efficient and secure business practices.
- By using B2B EC, business can reengineer their supply chain and partnership. B2B will offer access to following types of information.
    - **Product**-price, sales history.
    - **Customers**-sales history and forecast
    - **Suppliers** –product line and lead-time, sales terms and conditions.
    - **Product** process –capacity, product plan.
    - **Competitors** –market share, product offerings.
    - **Sales and marketing** –promotions.
    - **Supply chain process**-quality, delivery time etc.

What is a B2B exchange?

B2B exchange is a website we where many companies can buy from and sell to each other using a common technology platform. Many exchanges also offer addition services, such as payment or logistics services that help members complete a transaction. Exchanges may also support community activities, like distributing industry news, sponsoring online discussions and providing research on customer demand or industry forecasts for components and raw materials.

Development of B2B e-commerce

B2B e-commerce as a development process made up of a number of stages. At present this can typically be broken down into these five states:

- **Stage 1:** The business has interest in getting on-line, can see that it could bring competitive advantage and is increasingly aware of the need to maintain competitive parity. The company doesn‘t use e-mail and has neither internet access nor a company web site.
- **Stage 2:** The internet is being used as a marketing and communications tool. There is a company web site for increasing their marketing reach and the Net is used to gather information regarding possible competitors and suppliers. E-mail is widely used among partners but there is no link between any web activity and existing back office systems.
- **Stage 3:** The business uses the internet to interact with their customers. Their use of e-commerce has developed to the point where they are offing a full service storefront and possibly an online account management facility. Stage three is frequently split into two, with some companies stopping at the online store and not providing any integration into their back office systems for whatever reason. However stage three can only be said to be fully implemented when such integration has been achieved.
- **Stage 4:** This can almost be seenas an internally facing development as the business uses internet technologies to extend integration. Everything from their online shop front through to manufacturing and fulfillment is brought together and information can be gathered from all parts of the business. This allows the company to move towards a more integrated, on-line relationship with trading partners.
- **Stage 5:** The business joins online exchanges-marketplace and related services using the internet to connect then with business partners, suppliers and customers. At this point they could consider themselves to be part of a full B2B e- commerce scenario.

Type of B2B market

- **Supplier Oriented e-marketplace** - In this type of model, a common marketplace provided by supplier is used by both individual customers as well as business users. A supplier offers an e-store for sales promotion.
- **Buyer Oriented e-marketplace** - In this type of model, buyer has his/her own market place or e-market. He invites suppliers to bid on product's catalog. A Buyer company opens a bidding site.
- **Independent e-marketplace** - In this type of model, an intermediary company runs a market place where business buyers and sellers can transact with each other.
- **Vertical and horizontal e-marketplace**
    - Vertical e-marketplaces address the requirement of a specific industry sector such as automotive, chemical, construction, or textiles. A large organisation may set up such a marketplace to enable it to work with smaller business in its

supply chain, since it offer the potential to lower some of the high overheads to associate with working with a smaller supplier.

- A horizontal marketplace addresses regional or functional requirements. Companies use such marketplaces to purchase indirect products such as office equipment or stationery.

Classifying B2B Hubs

This simple two-way classification - manufacturing inputs versus operating inputs (the ―what business buy‖); and systematic sourcing versus spot sourcing (the ―how business buy‖) allows us to classify B2B hubs into four categories

- MRO hubs (operating supplies, systematic sourcing, horizontal focus)
- Yield managers (operating supplies, spot sourcing, horizontal focus)
- Catalog hubs (manufacturing inputs, systematic sourcing, vertical focus)
- Exchanges (manufacturing inputs, spot sourcing, vertical focus)

Manufacturing inputs:

These are raw materials and components that go directly into the products or process

Operating inputs:

These are not parts of finished goods but include things like office supplies, spare parts, and airline tickets. These are often called maintenance, repair and operating (MRO) goods.

Systematic sourcing:

This involves negotiated contracts. These arrangements involve long-term relationship between buyer and seller. Spot sourcing: In this case buyer's objectives to fulfil an immediate need at the lowest possible cost. This does not involve any long-term relation between buyer and seller.

MRO hubs

These hubs concentrate on goods with low values. The transaction cast is relatively higher. These hubs provide value by increasing the efficiency in the procurement process. These hub use third party logistics supplier to deliver goods, thus enabling them to disintermidiate or bypass existing middlemen in the channel. Examples of hub are MRO.com, bizbuier.com and Ariba.

Yield manager:

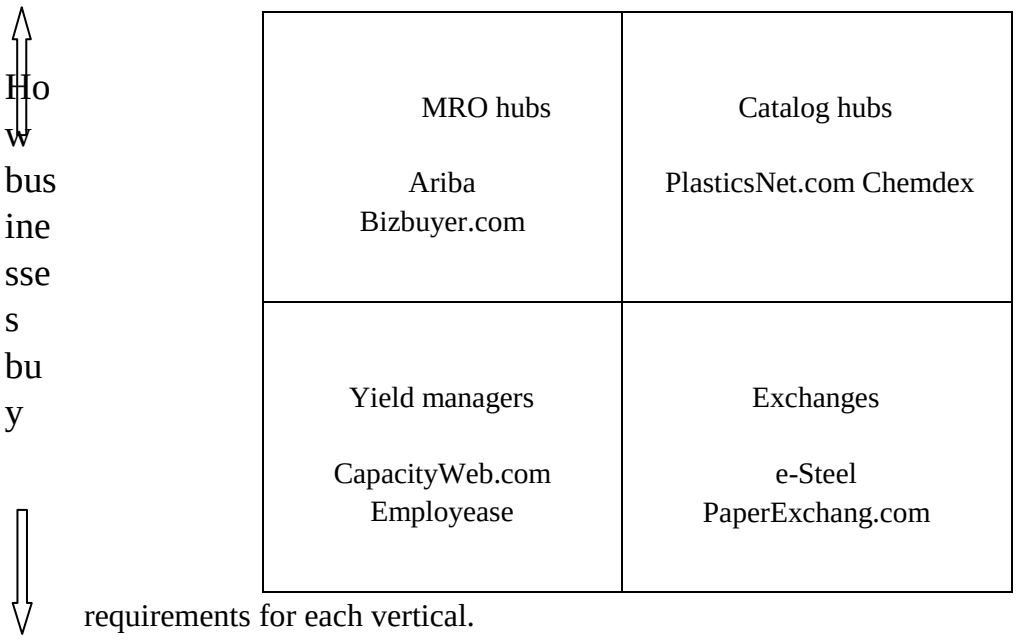
Yield managers focus on the spot procurement of operating inputs. These yield managers aim to insulate buyers and sellers from ups and downs in operations by allowing them to scale their operating resources upwards or downwards at short notice by participating in the spot market. They add most value in situations where there is high degree of price and demand volatility (e.g., utilities), or where there are huge fixed-cost assets that cannot be liquidated or acquired at short notice. Yield managers tend to be more vertical in nature than MRO hubs, but are less vertical in nature than industry-specific vertical hubs like Chemdex or PlasticsNet.com. Examples of hub are utility sector, employease, elance for human resources, and iMark for capital equipment and capacity web for manufacturing.

Exchanges:

Exchanges aim to create spot markets for commodities or near-commodities within specific industry verticals. These exchanges approximate commodity exchanges, and largely focus on transactional sourcing. The exchange maintains relationships with buyers and sellers, but buyers and sellers rarely have direct relationships. In fact, in many exchanges, buyers and sellers may not even know each others' identities. Exchanges serve a yieldmanagement role, because they allow purchasing managers to smooth out the peaks and valley in demand and supply by ―playing the spot market‖. Examples of exchanges include E-Steel, PaperExchange, and IMX Exchange.

Catalog units:

Catalog hubs streamline the systematic sourcing of manufactured input within specific vertical industries. These players start out by putting industry-specific catalogs online, and creating a large universe of supplier catalogs within the vertical. They aim to automate the systematic sourcing process, and create value for buyers by lowering transaction costs. These catalog hubs can be buyer-focused or seller-focused, depending upon who they create more value for. Examples include PlasticsNet.com, Chemdex, and SciQuest. Catalog hubs need to work closely with distributors, especially on specialized fulfilment and logistics



requirements for each vertical.

sourcing

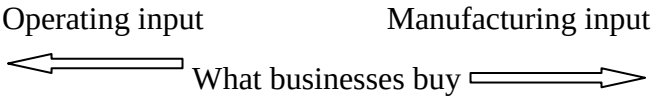


Fig.2.4. B2B Matrix

E-hubs create value using two fundamentally different mechanisms: aggregation and matching.

Aggregation

The aggregation mechanism relies on bringing a large number of buyers and sellers under one roof, and reducing transaction costs by ―one-stop shopping‖. For example, PlasticsNet.com allows plastics processors to issue a single purchase order for hundreds of plastics products, and PlasticsNet.com sources these products from a diverse set of suppliers.

An important characteristic of the aggregation mechanism is that adding another buyer to the hub only benefits sellers, and does not benefit other buyers. This happens for a simple reason – buyers can never be sellers in a catalog aggregation model. So adding a buyer to the system only benefits sellers, and adding a seller to the system only benefits buyers.

Matching

The matching mechanism is a trade mechanism that creates value by bringing buyers and sellers together to negotiate prices on a dynamic and real-time basis. For example, iMark.com brings buyers and sellers together in the market for used capital equipment. In contrast with the aggregation mechanism, buyers can be sellers in the matching mechanism. So adding a buyer to the hub benefits buyers as well as sellers.

Private exchanges:

In these exchanges company connect with its supplier base or customer base. It is one to many connections between the company and its trading partners. In private exchange companies do not look beyond their existing customer /supplier base. These exchanges provide deep collaboration and focus on direct material procurement capabilities and have sophisticated e-market capabilities, develop through use of advance software application and integration with trading partners ERP systems. Private exchange offer privacy, security and superior collaborative capabilities.

Industry consortium:

This model provides some to many connection among industry members and their trading partners. These e-markets give individual members industry members and their trading partners. These exchanges also offer collaborative capabilities as private exchanges. Industry consortium serve large customer base.

Independent market:

This type of e-market brings buyers and seller come together. This is many-to-many connection among buyers and sellers. This market has widest variety of participants, but makes collaboration difficult. These exchanges focus on low risk activities like MRO and indirect material many independent markets will offer trust building services like supplier rating, created verification.

B2B e-commerce needs to focus on broader set of activities in supply chain management, supply chain need to move away from simple actions & procurement capabilities. It needs to move toward more collaborative supply chain planning & execution automation for indirect & direct materials.

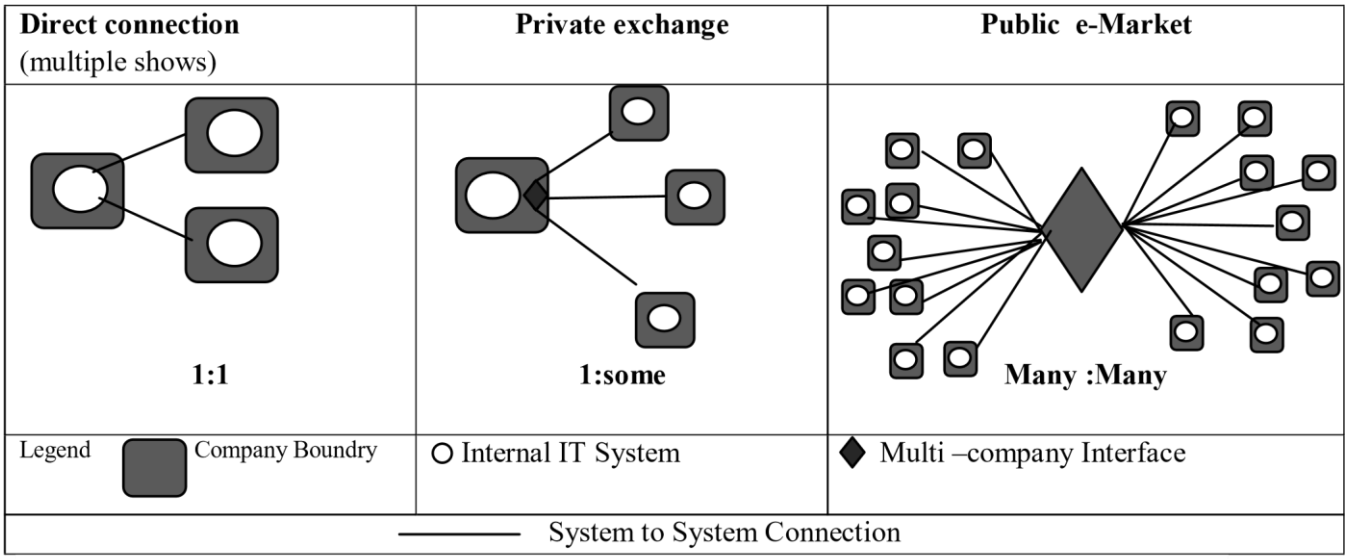


Fig. 2.5. B2B Connectivity model

E-HUB

An e-Hub is web enabled platform that allow trading partners to find , exchange & share information related to buying & selling activities. Various transactions whether inbound or outbound required in customer order fulfilment are automated.

It provides complete transparency at all stages of execution of a transaction. Execution of incoming customer transaction from ―far up‖ in the channel to contract manufacturer in the supply chain is automated.

The ehub is more suited for supply chain collaboration as ehub is accessible to several different parties; all parties contribute their share of information to create a pool of dynamic

information at ―mission control center‖ in the ehub. Since all trading partners can tap into this information it serves multiple functions. It provides not only current view of the order but also provides visibility into other aspects of fulfilling that order, such as production capacity, inventory availability and logistic and fulfilment status.

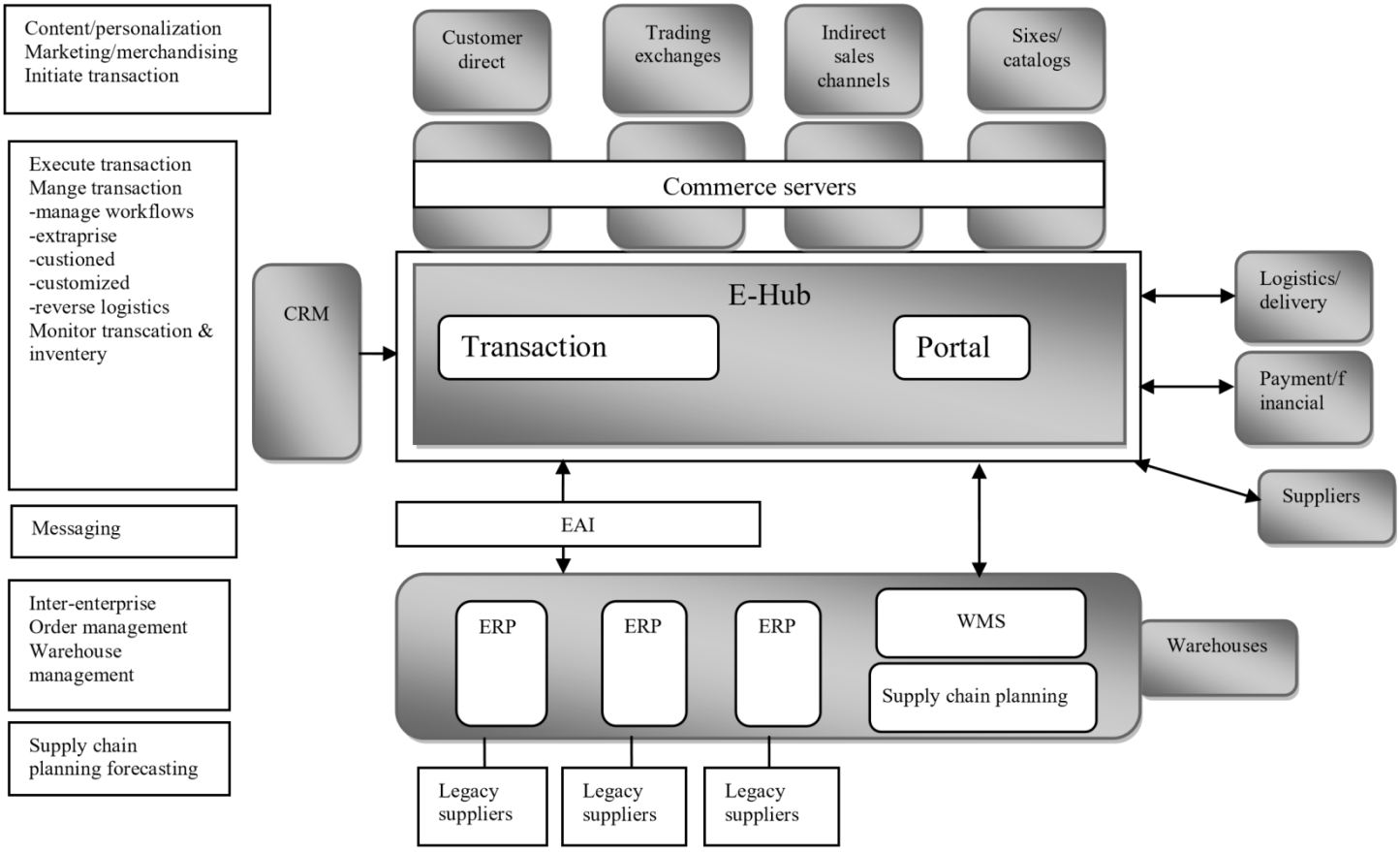


Fig. 2.6. E-HUB

Capabilities & Functionalities of e-Market:

E-marketplaces should provide the participants with an open, flexible, reliable, highly available and scalable environment. It should have functionalities & capabilities that

Capabilities:-

- E-markets are not only bringing trading partners together but also competitors.
- Private exchanges bring together trading partners while industry consortium bring together industry competitors is to share information, increase collaboration to increase the bottom line and provide greater value to business shareholders.

- Competitors are working together with other competitors to determine market demand, and share information to increase the efficiency across the entire supply chain.
  - E-market should promote multi partner collaborative capabilities.
- They should enable collaboration in inventory management, planning &scheduling.
- Activities like collaborative product design have become possible as a result of exchange capabilities.
- E-market should have EAI (Enterprise Application Integration) capabilities.
- This will allow even incompatible legacy systems to integrate with the e-market using some translation technology like EDI, middleware or XML.

Functionality:-

E-market should provide functionality & services. Specialized functionality & service may be developed for private exchanges, which are more closely centred on a company and its trading partners.

- Scalability/availability:

  E-market should have capabilities to handle large volume of data. A proper IT infrastructure should be in place to ensure load handling and availability of services. Availability if services are 24 X 7 X 365.

- Security:

  The e-market should have capabilities to provide secure transaction processing for its customers. Technologies like encryption, SSL or validation keys are few technologies that can be used. Proper authentication and authorization procedures should be in place. Security can be a make-or-break issue.

- Privacy:

  Privacy policies should be in place and effectively implemented. Companies do not want to share their proprietary information with anyone.

- Content/catalog management:

  Capability to create and manage web site elements such as text graphics, embedded files and applets is important aspects. Web site should be user friendly and easy to navigate.

- Hub & spoke architecture:

Developing and building on an open architecture, where players can easily be added, removed and experience growth is very important functionality that an e-market should have.

Relationship of B2B e-commerce with other perspectives:

❖**Electronic marketing**-

B2B platform can be used to sell the company‘s product and services to business customers on the internet.

This model can be called seller oriented marketing because customers visit the web site that the supplier has prepared.

❖**Procurement management**-

B2B is a medium of facilitating procurement management such as reduced prices and reduced cycle time.

To implement b2b from the procurement management point of view the buyeroriented market place can be used where the buyer announces the RFQ to the potential suppliers for competitive purchasing.

To the suppliers, participating to the customers oriented marketplace & winning the bid is the major concern.

❖**Electronic intermediaries**-

Individual consumers & business purchases a group of items such as books, stationary and personal computers, in such cases the consumers and business buyers can share the intermediary.

Since purchasing party is a business that has to deal with many suppliers and intermediaries.

❖**Just in time**-

JIT delivery of parts to manufacturing buyers is crucial to realize JIT manufacturing.

Direct marketing requires an internal JIT manufacturing system, the JIT delivery and advanced confirmation of supplier‘s inventory are essential elements for B2B.

❖**EDI-**

EDI is the electronic exchange of specially formatted standard business documents such as orders, bills approval of credit, shipping details and confirmation sent between business partners.
The EDI translator is necessary to convert the proprietary data into standard format.
Internet based EDI is an important technology for B2B e-commerce.

Impact of B2B on business processes:

Procurement processes

- Almost half of companies in the survey said they were in the earliest state of using the internet for purchasing. The larger organisations were more likely to have purchased online and to have experienced major benefits from doing so and 27% claimed they had actually saved money. The percentage of business carried out this way was still small, with only 6% of the companies completing more than 40% of their purchasing online.
- Innovative product & service suppliers hoping to move into B2B have found problems understanding the complex relationship that exists in the supply chain scenario & are increasingly looking towards suppliers who have traditionally operated.
- Suppliers have found that the purchase of direct materials is much more complex than indirect.

Fulfilment

- Fulfilment depends on what products or services are being sold & indeed smaller companies, with an easy-to-deliver product, can obtain significant new business opportunities.
- The companies involved in B2B deliveries have an advantage over those involved in B2C trading.
- They can design efficient routes fairly easily since business customers tend to be clustered in areas.
- Shipments are typically much larger and consequently, B2B shipments are usually two-to-three times less expensive than B2C deliveries.

Managing trading partner relationships

- The effective use of e-commerce can have a significant impact on trading partner relationships.
- B2B e-commerce is a significant enabler in their move towards greater trading partner collaboration.
- Services can be customised to meet individual trading partner needs.
- This includes the provision of effective communications about the status of orders and delivery, together with the speedy resolution of queries and post sales support issues.

Benefits of B2B E-Commerce

- Managing inventory more efficiently
- Adjusting more quickly to customer demand
- Getting products to market faster
  - Cutting the cost of paperwork
  - Reigning in rogue purchases
  - Obtaining lower prices on some supplies

2.5 Difference between B2C and B2B

There are 12 major differences between B2B ecommerce and B2C ecommerce that are

	B2C	B2B
Market	Broad & General	Small & Targeted
Goals	Product Driven	Relationship Driven
Buying Process	Short & Sweet	Multi-Step, Complex
Users	Consumers	Sales Reps, Brokers, Dealers, Others
Frequency	Typically One-Time	Typically Repeat Orders
Order Total	Typical Low Price	Typically High Price
Stock Status	Typically in-stock	Often not in stock
Order Creation	Manual or Disconnected	Automated Order Creation in ERP
Pricing Strategies	Standard Pricing	Complex, Specific Pricing by Customer
Payments	Typically Credit Card	Typically On Account Credit Sales
Fulfillment	Often 3rd Party Warehouse	Typically Internal Warehouse
Shipping	Common Carriers	Common Carrier, LTL, TL, Other

Fig. 2.7.B2B Vs B2C

2.6 Consumer-to-Consumer (C2C) Model

The C2C model involves transaction between consumers. Here, a consumer sells directly to another consumer. eBay and www.bazee.com are common examples of online auction Web sites that provide a consumer to advertise and sell their products online to another consumer.

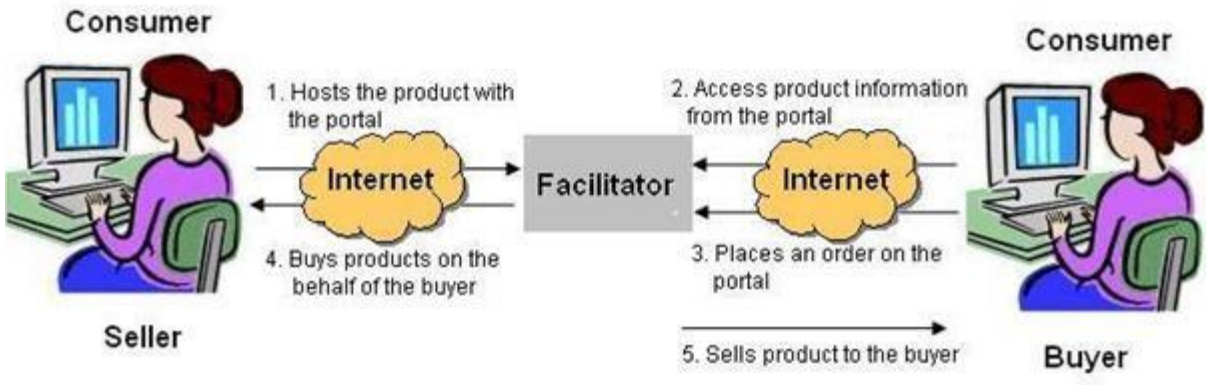


Fig 2.8. C2C business model

OTHER MODELS:

Consumer-to-Business (C2B) Model

The C2B model involves a transaction that is conducted between a consumer and a business organization. It is similar to the B2C model, however, the difference is that in this case the consumer is the seller and the business organization is the buyer. In this kind of a transaction, the consumers decide the price of a particular product rather than the supplier. This category includes individuals who sell products and services to organizations. For example, www.monster.com is a Web site on which a consumer can post his bio-data for the services he can offer. Any business organization that is interested in deploying the services of the consumer can contact him and then employ him, if suitable.

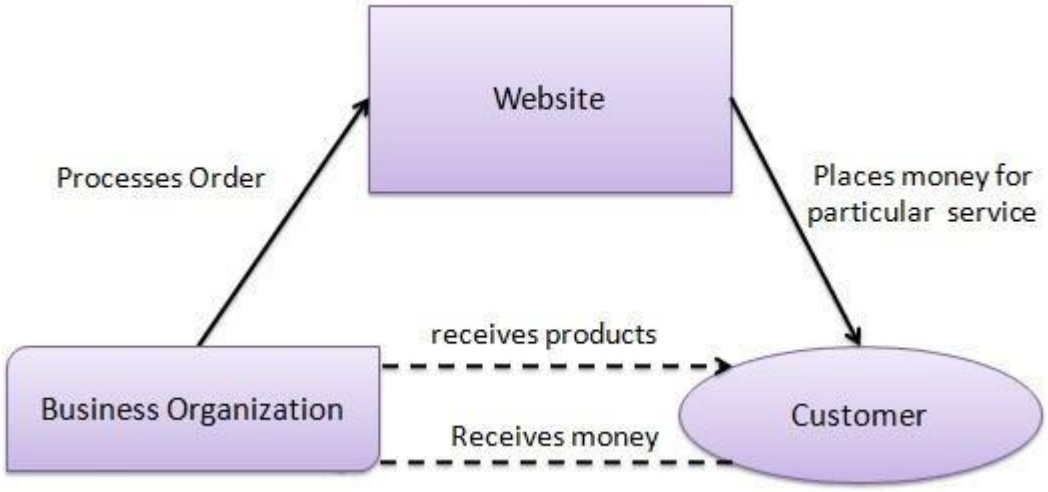


Fig. 2.9. C2B Business Model

Business-to-Government (B2G) model

The exchange of information, services and products between business organisations and government agencies on-line. This may include,

- **E-procurement services**, in which businesses learn about the purchasing needs of agencies and provide services.
- **A virtual workplace**in which a business and a government agency could coordinate the work on a contracted project by collaborating on-line to coordinate on-line meetings, review plans and manage progress.

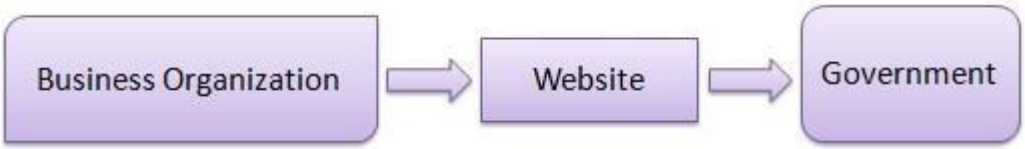


Fig. 2.10. B2G Business Model

CHAPTER - 3
B2B E-COMMERCE AND EDI

Business to Business (B2B) is the means of conducting business between two or more companies over the internet, it involves business dealing with each other as opposed to their customers.

3.2 Need for B2B

- It allows the business to replace a number of people in their works department with automated systems.
- It substantially reduces business cycle time.
- It helps in running the business more efficiently, quickly and securely.
- Managing inventory more efficiently.
- Adjusting more quickly to customer demand.
- Getting products to market faster.
- Cutting the cost of paperwork.
- Reigning in rogue purchases.
- Obtaining lower prices on some supplies.

3.3 EDI(Electronic Data Interchange):

- EDI stands for Electronic data interchange. It is the application to application transfer of Business documents between computers. The transfer of files requires that the sender and receiver agree upon a standard document format for the document that is to be transmitted.
- EDI is a new way of doing business. Many businesses are looking to EDI as a new, fast, inexpensive, and safe method of sending purchase orders, invoices, shipping notices, receiving advices, and other frequently used business documents.
- EDI can also be used to transmit financial information and payment in electronic form. When used in this application, EDI is usually referred to as financial EDI or Electronic Fund Transfer (EFT).
- EDI is the direct interchange of business documents such as invoices, bills, orders etc. between two organizations through computers.
- It saves money and time as the processing is very fast through the telecommunication network between the different businesses.
- It eliminates the tedious task of printing and handling of paper on one hand and input of the data on the other.

3.4 Paperless Transaction

- EDI differs from electronic mail because it transmits an actual structured transaction in contrast to an unstructured text message such as a letter. By minimizing the amount of time used in the inventory, it also helps in minimizing the costs.

- In the case of working with EDI, physical movements of paper are avoided and time per each movement can be reduced since all these activate are computer to computer exchange.
- Organizations can most benefit from EDI when they integrate the data supplied by EDI with applications such as accounts payable, inventory control, shipping and production planning.

For proper working of EDI model, there are four key requirements:

- Transaction formats and data should be standardized.
- Special software should be developed for converting the message into a form suitable to other companies.
- There should be value added network with mail box facilities among the companies following the EDI. It would allow the messages to be, sorted and held until they are needed by the receiving computer.
- Certain transaction would still require the writing in hard copy form. This may be due to legal requirements.

Company uses EDI to automate price, shipping, receiving and payment transactions with its customers. Price updates and shipping notices are entered by the appropriate departments directly into company‘s material releases, receiving reports and payment data are also transmitted directly through the computer system back to the company. EDI has replaced paper for these transactions.

Components of EDI:

- **Trade agreement –** a legally binding trade agreement between you and your trading partner.
- **Standard document format –** the Standard agreed upon format for document to be electronically transmitted.
- **EDI Translation management software –** software used to convert the document your application‘s format into the agreed upon standard format. For optimum performance the translation software should be on the same platform as your business application.
- **Communications software –** a programming tool that enable you to write communications protocols, or a separateapplication.
- **Modem –** a hardware device used to transmit electronic between computer systems.
- **Van –** stands for value added network. A network to which you can connect to transmit data from one-computer system to another.
- **Point-to- Point –** a direct communication link from one computer system to another. Some trading partners offer a direct connection to their EDI computer.

Features of EDI:

1. It is highly secure.

2. It offers speed.
3. It is reliable.
4. It will put you in a better market position in relation to non-EDI competitors.

EDI Model:

- This involves two or more trading partners who want to exchange data from the organizations (may be customer and supplier).
- There may be two companies with a common customer or two banks whose customers want to deal with one another.
- Trading partners will have the flow of data between them through exchanges. The simplest and the most common form of exchange is where one partner wants to send a single message to the other and to know whether the other one has received the message or not.
- The message if passed successfully and reliably from one partner to another, it is said that EDI is operated. There a may be one message to reach several destinations also, through the protocol of EDI does not permit this.

3.5 EDI standards

In the early days of EDI large firms announced a proprietary format and communication interface and either encouraged or mandated trading partner participation.

Electronic Data Interchange Association (EDIA) was instrumental in developing standards and providing education and support in the use of EDI.

It was replaced by Data Interchange Standards Association (DISA) current secretariat for American National Standards Institute Accredited Standards Committee (ANSI ASC X12), the EDI standards organization in the United States.

ANSI is the US representative to the International Standards Organization (ISO).

3.6 Data Standards used in EDI

The two data standards commonly used in EDI system are:

- Data encryption standards (DES)
- Rivert-shamier-adelmann (RSA)

DES:

It was developed by IBM for the U.S. department of defence and was later on published as a standard. The same key is used both for encryption and decryption of the messages.

RSA:

It was developed by a group of mathematicians who believed that it would not be possible to devise a code that could be deciphered using a public key without giving away the encryption key.

3.7 Cost of EDI

Prices for EDI applications vary from free to several thousand for full-function applications. The final price will pay depends upon several things:

- The expected volume of electronic document.
- The amplitude of the EDI translation software.

- Maintenance fees.
- VAN charges.
- Mailbox costs.
- Implementation costs.
- Running costs.
- Study and decision making.
- Other reorganization costs.

3.8 Reasons for Slow acceptability

➢Too many standards

There are too many standards bodies developing standards documents formats for EDI.

➢Changing standards

Each year, most standards bodies publish revision to the standards. This poses a problem to EDI users. You may be using one versions of the standard while your trading partners are still using older versions.

➢EDI is too expensive

Some companies are only doing business with other who uses EDI. If a company wants to do business with these organizations, they have to implement an EDI program. This expense may be very costly for small companies.

➢Limit your trading partners

Some largecompanies tend to stop doing business with companies who don‘t comply with EDI.

3.9 Electronic Fund Transfer

The EFT encompasses any monetary transaction that is completed by electronic means; i.e. automated teller machine (ATM) transactions, wire transfers, point of sale (POS) transactions, and tape exchange of financial data.

This report will focus on the coupling of EFT with Electronic data interchange (EDI) technologies - where EDI refers to computer- to- computer Electronic exchange of business document such as purchase order and shipping notices between business partner‘s, in a computer readable format.

<u>Combination EDI and EFT:</u>

By combining EFT with the advantages provided by EDI business gain in many ways:

1. Reduce time spent in data entry, paper processing and error correction, by having your accounts payable system directly feed your EDI translator.
2. Reduce/eliminate the costs associated with cheque preparation, enveloping, mailing, cheque reconciliation, storage and retrieval by creating and sending payments electronically to the bank.
3. Accurate cash flow forecasting for these payments, and improve control of overall cash flow because the transfer of funds are guaranteed on value date. This also allows you to advantages of discounts by establishing set payment dates.

4. No time is due to mail and processing float, as payment can be sent from anywhere.
5. Reduce time, error, and cost of handling incoming cheque, bank deposits and data entry into your accounts receivable system.

The role of banks in EDI:

- Banks are the only organizations that can process any sort of money transaction.
- If two companies wish to enter into an EDI partnership, they may directly transfer all ordering and invoice information directly between each other, but any transfer of funds must be made via an electronic request to a bank.
- Upon receipt of this request, the bank may either transfer the funds directly (if both companies use the same bank) or go through appropriate channel to settle with another bank.

3.10 XML and its application

- XML (Extensible Markup Language) is a general-purpose specification for creating custom markup languages.
- The term extensible is used to indicate that a markup-language designer has significant freedom in the choice of markup elements.
- XML's goals emphasize representing documents with simplicity, generality, and usability over the Internet.
- XML has been used as the basis for a large number (at least hundreds) of customdesigned languages. Some of these, for example RSS, Atom, and XHTML, have become widely used on the Internet.
- XML dialects (often packaged in archive files) are becoming the default file format for office-productivity software packages, includingMicrosoftOffice, OpenOffice.org, AbiWord, and Apple's iWork.

Applications of XML

- The graphical user interface provided with OpenStage 60/80 phones can be used to develop own applications for special purposes. **XML applications** enable the phone to act as a front-end to a server-side program. Moreover, XML applications have the capability of controlling calls.
- The *Push* feature allows the server-side program to send data to the phone in an unsollicited manner. The information is displayed immediately on the phone. Possible uses are, for instance: Integration with groupware (e.g. Microsoft Exchange Server) or Unified Messaging systems (e.g. Siemens OpenScape); gathering information provided by web services (e.g. weather, traffic, stocks); dialing aids with access to address databases.

3.11 Comparison of HTML and XML

- HTML was designed to display data with focus on how data looks while XML was designed to be a software and hardware independent tool used to transport and store data, with focus on what data is.
- HTML is a markup language itself while XML provides a framework for defining markup languages.
- HTML is a presentation language while XML is neither a programming language nor a presentation language.
- HTML is case insensitive while XML is case sensitive.
- HTML is used for designing a web-page to be rendered on the client side while XML is used basically to transport data between the application and the database.
- HTML has its own predefined tags while what makes XML flexible is that custom tags can be defined and the tags are invented by the author of the XML document.
- HTML is not strict if the user does not use the closing tags but XML makes it mandatory for the user the close each tag that has been used.
- HTML does not preserve white space while XML does.
- HTML is about displaying data, hence static but XML is about carrying information, hence dynamic.

3.12 Advantage of XML as a Technology

- It is a platform independent language.
- It is as easy as HTML.
- XML is fully compatible with applications like JAVA, and it can be combined with any application which is capable of processing XML irrespective of the platform it is being used on.
- XML is an extremely portable language to the extent that it can be used on large networks with multiple platforms like the internet, and it can be used on handhelds or palmtops or PDAs.
- XML is an extendable language, meaning that you can create your own tags, or use the tags which have already been created.
- It can be deployed on any network if it is amicable for usage with the application in use. If
- the application can work along with XML, then XML can work on any platform and has no boundaries.
- It is also vendor independent and system independent. While data is being exchanged using XML, there will be no loss of data even between systems that use totally different formats.

- **Disadvantages of XML**
- More difficult, demanding, and precise than HTML.
- Lack of browser support/ end user applications.

Still experimental/not solidified.

Design Goals of XML

The design goals for XML are:

- XML shall be straightforwardly usable over the Internet.
- XML shall support a wide variety of applications.
- XML shall be compatible with SGML.
- It shall be easy to write programs which process XML documents.
- The number of optional features in XML is to be kept to the absolute minimum, ideally zero.
- XML documents should be human-legible and reasonably clear.
- The XML design should be prepared quickly.
- The design of XML shall be formal and concise.
- XML documents shall be easy to create.
- Terseness in XML markup is of minimal importance.

Structure of XML document

Here's a complete (but very simple) XML document:

```
<?xml version="1.0"?>

<contact-info>
<name>Jane Smith</name>
<company>AT&amp;amp;T</company>
<phone>(212) 555-4567</phone></contact-info>
```

There are two different kinds of information in this example:

1. **markup**, like ―<contact-info>‖ and ―&‖; and
2. **text** (also known as **character data**), like ―Jane Smith‖ and ―(212) 555-4567‖.

XML documents mix markup and text together into a single file:

- ✓ The markup describes the structure of the document,
- ✓ While the text is the document's content (actually, sometimes markup can also represent content, as in the case ofreferences: more on this point below).

Here's the same XML document again, with the markup highlighted to distinguish it from the text:

<?xml version="1.0"?>

<contact-info><name>Jane Smith**</name><company>**AT**&**T**</company><phone>**(212) 555-4567**</phone></contact-info>**

Let‘s discuss how to use different kinds of markup and text in an XML document:

- the XML
- declaration;tags and
- element;attributes;ref
- erences; and text.
-

XML Declaration

All XML documents can optionally begin with an **XML declaration**. The XML declaration provides at a minimum the number of the version of XML in use:
<?xml version="1.0"?>

Currently, 1.0 is the only approved version of XML, but others may appear in the future.

The XML declaration can also specify the character encoding used in the document:

<?xml version="1.0" **encoding="UTF-8"**?>

All XML parsers are required to support the Unicode ―UTF-8‖ and ―UTF-16‖ encodings; many XML parser support other encodings, such as ―ISO-8859-1‖, as well.

There a few other important rules to keep in mind about the XML declaration:

- The XML declaration is case sensitive: it may not begin with ―<?XML‖ or any other variant;
- If the XML declaration appears at all, it must be the very first thing in the XML document: not even whitespace or comments may appear before it; and
- It is legal for a transfer protocol like HTTP to override the encoding value that you put in the XML declaration, so you cannot guarantee that the document will actually use the encoding provided in the XML declaration.

Tags and elements

XML tags begin with the less-than character (―<‖) and end with the greater-than character (―>‖). You use tags to mark the start and end of **elements**, which are the logical units of information in an XML document.

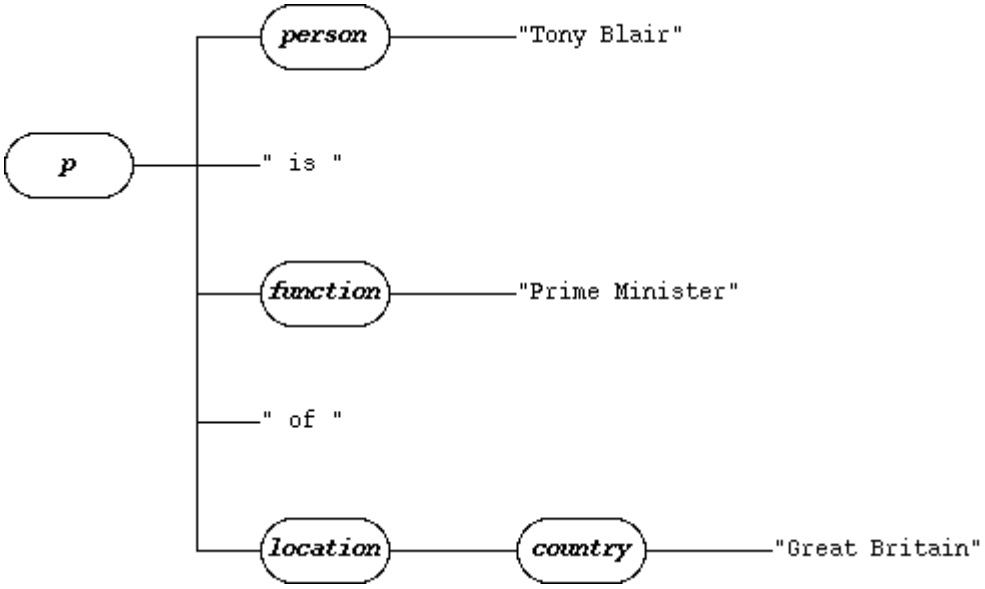
An element consists of a **start tag**, possibly followed by text and other complete elements, followed by an **end tag**. The following example highlights the tags to distinguish them from the text:

** <person>**Tony Blair**</person>** is **<function>**Prime Minister**</function>** of **<location><country>**Great Britain**</country></location> **.

Note that the end tags include a solidus (—/‖) before the element's name. There are five elements in this example:

- The *p* element, that contains the entire example (the *person* element, the text — is ‖, the *function* element, the text — of ‖, and the *location* element);
- The *person* element, that contains the text —Tony Blair‖;
- The *function* element, that contains the text —Prime
- Minister‖; The *location* element, that contains the *country*
- element; and The*country* element, that contains the text —Great Britain‖.

The following illustration shows this structure as a tree, with *p* (the outermost element) at the root:



There are a few rules to keep in mind about XML elements:

- Elements may not overlap: an end tag must always have the same name as the most recent unmatched start tag. The following example is not well-formed XML, because —</person>‖ appears when the most recent unmatched start tag was —<function>‖:
- <!-- WRONG! -->
- **<function><person>**President**</function>**Habibe**</person>** The

following example shows the tags properly nested:

<person><function>President**</function>**Habibe**</person>**

- An XML document has *exactly* one root element. As a result, the following example is not a well-formed XML document, because both the *a* and *b* elements occur at the top level: <!-- WRONG! -->
-
-
-

<a>...
...

The following example fixes the problem by including both the *a* and *b* elements within a new *x* root element:

<x>
<a>...
...
</x>

- XML element (and attribute) names are case-sensitive, so ―location‖ and ―Location‖ refer to different elements. This is a very nasty trap for people used to working with HTML or other SGML document types, because it can cause surprising bugs in processing software, or can even lead to malformed XML documents, as in the following example:
- <!-- WRONG! -->
- <a href="pbear.html">polar bear</A>

This example will cause a parser error because an XML processor considers *a* and *A* to be separate elements, so the start and end tags do not match.

In some cases, an element may exist that has no content (for ex, the HTML *hr* element), but the tag is still read by processors. Rather than type a start and end tag with nothing between them (for example, ―<hr></hr>‖), XML has a special **empty-element tag** that represents both the start tag and the end tag:

Stuff<hr/>
More stuff.

In this example, ―<hr/>‖ represents both the start and the end of the *hr* element; it could just as easily have been written as ―<hr></hr>‖ (which is exactly equivalent).

Attributes

In addition to marking the beginning of anelement, XML start tags also provide a place to specify **attributes**. An attribute specifies a single property for an element, using a name/value pair. One very well known example of an attribute is *href* in HTML:

Yahoo!

In this example, the content of the *a* element is the text ―Yahoo!‖; the attribute *href* provides extra information about the element (in this case, the Web page to load when a user selects the link).

Every attribute assignment consists of two parts: the **attribute name** (for example, *href*), and the **attribute value** (for example, http://www.yahoo.com/). There are a few rules to remember about XML attributes:

- Attribute names in XML (unlike HTML) are case sensitive: *HREF* and *href* refer to two different XML attributes.
- You may not provide two values for the same attribute in the same start tag. The following example is not well-formed because the *b* attribute is specified twice:
- ....
- Attribute names should never appear in quotation marks, but attribute values must always appear in quotation marks in XML (unlike HTML) using the " or ' characters. The following example is not well-formed because there are no delimiters around the value of the *b* attribute:
- <!-- WRONG! -->
- ...

You can use the pre-defined entities —"‖ and —'‖ when you need to include quotation marks within an attribute value.

Some attributes have special constraints on their allowed values: for more information, refer to the documentation provided with your document type.

References

A **reference** allows you to include additional text or markup in an XML document.
References always begin with the character —&‖ (which is specially reserved) and end with the character —;‖.

XML has two kinds of references:

Entity references

An entity reference, like —&‖, contains a name (in this case, —amp‖) between the start and end delimiters. The name refers to a predefined string of text and/or markup, like a macro in the C or C++ programming languages. **Character references**

A character references, like —&‖, contains a hash mark (—#‖) followed by a number. The number always refers to the Unicode code for a single character, such as 65 for the letter —A‖ or 233 for the letter —‖, or 8211 for an en-dash.

For advanced uses, XML provides a mechanism for declaring your own entities, but that is outside the scope of this tutorial. XML also provides five pre-declared entities that you can use to escape special characters in an XML document:

Character	**Predeclared Entity**
&	&amp;
<	&lt;
>	&gt;

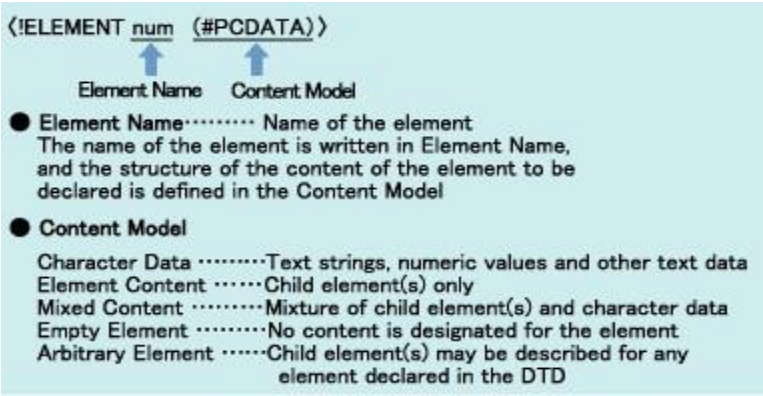
" "

' '

For example, the corporate name ―AT&T‖ should appear in the XML markup as ―AT&T‖: the XML parser will take care of changing ―&‖ back to ―&‖ automatically when the document is processed.

Document Type Definition (DTD)

A Document Type Definition (DTD) defines the legal building blocks of an XML document. It defines the document structure with a list of legal elements and attributes. A DTD can be declared inline inside an XML document, or as an external reference. **Declaring elements in DTD**



Element Type

Empty:-Empty elements have no content and are marked up as <empty-elements>

Unrestricted: - The opposite of an empty element is an unrestricted element, which can be contain any element declared elsewhere in the DTD.

Symbol	Meaning	Example	Description
+	It indicates that there can be at least one or multiple occurrences of the element.	Course +	There can be multiple occurrences of course element.
*	It indicates that there can be either zero or any number of occurrences of the element.	Content *	Any number of content elements can be present.
?	It indicates that there can be either zero or exactly one occurrence.	Content ?	Content may not be present or present only once.
|	Or	City | state	City or state

Attribute Type

Type	Description
Required	If attribute of an element is specified as # REQUIRED then the value of that attribute must be specified if will not be specified then the xml document will be invalid.
Fixed	If an attribute of an element is specified as #FIXED then the value of attribute can not be changed in the xml document.
Implied	If attribute of an element is specified as #IMPLIED then attribute is optional i.e. this attribute need not be used every time when its associated element is used.

For example, while we haven't gone over the structure of a DTD yet, here is part of a simple one. It states that there is a root element called "family" that has two possible elements within it: "parent" and "child":

```
<!DOCTYPE family [
<!ELEMENT parent (#PCDATA)>
<!ELEMENT child (#PCDATA)>
]>
```

If you were to write an XML document based upon that DTD, you could write:

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE family [
<!ELEMENT parent (#PCDATA)>
<!ELEMENT child (#PCDATA)>
]>

<family>
<parent>Judy</parent>
<parent>Layard</parent>
<child>Jennifer</child>
<child>Brendan</child>
</family>
```

This would be a valid XML document. But if I added extra text outside of the <parent> or<child> tags, the document would be invalid until I changed the DTD:

3.13 E-Marketing

E-marketing is the use of web-based applications and services to select and segment customers, develop and execute marketing campaigns.

E-marketing is a type of marketing that can be defined as achieving objectives through such as internet, e-mail, e-book, database, and mobile phone.

3.14 Online Marketing and its Strategies

It is a form of marketing that combines the traditional marketing principles with the interactive capabilities of internet.

In online marketing,

- Companies devised plans to attract online visitors to a website and encourage them to register or purchase products.
- Direct communication takes place in real time.

Different online marketing strategies are:

- **Search engine optimization (SEO):**

  The process of preparing web pages to be submitted to and ranked high in search engines (such as Yahoo!, Google, MNS, AOL, etc.).

- **Viral marketing (VM):**

  Viral marketing describes any strategy that encourages individuals to pass on a marketing message to others, creating the potential for growth in message‘s exposure and influence.

  Viral marketing is one of the most exciting and powerful ways to reach the audiences. It‘s not easy to harness the power of word-of-mouse, but any company with thoughtful ideas to share and clever ways to create interest in them, after some careful preparation, it becomes famous and success on the web.

- **Associate/affiliate programs:**

  Affiliates are companies, groups and individuals who promote advertisers.

  Affiliate marketing is an internet-based marketing practice in which a business rewards one or more Affiliate for each visitor or customer brought about by the Affiliate‘s marketing efforts.

  Affiliate marketing is a working relationship whereby a merchant (online shop or advertiser) has consumers driven to it by adverts on an Affiliate (website).

  If a consumer visiting the Affiliate‘s site clicks on an advertisement and goes on to perform a predetermined action (usually a purchase) on the advertiser‘s site then the Affiliate receives a payment.

  The Affiliate marketing industry has three core players at its heart: the brand/seller, the Affiliate, and the customer.

  Affiliate marketing overlaps with other internet marketing methods to some degree, because affiliates often use regular advertising methods. Those methods include organic search engine optimization, paid search engine marketing, e-mail marketing and display advertising.

3.15 Traditional options of Web Promotion

- **Banner Ads**

  Banner ads are rectangle boxesthatsiton a web page and, when clicked, send a visitor to the advertiser‘s web page. Animaed banners have higher click through rates than standard banners.

- **Banner Exchanges**

  Banner exchange program, where random sites run your banner and you run randon banner these sitesin return. guidelines differ between exchanges services, but this option shouldn‘t cost your money, only space on yur web page.

- **Ad Networks**

  Ad netwrk give you a targeted audience and updates about the success of your banner. When you work with an ad network you have two options.

  - Involves paying the network to place and monitr the success of your banner.
  - You allow them to publish ther banners on your website and they pay you .

  Both option gives the result.

- **Web Counter**

  A web counter or hit counter is a computer software program that indicates the numberofvisitiors, or hits, aparticular web page has received.Once set up these counters will be incremented by one every time the web page is acessed in a web browser. The counter should accompanied by the date it was set up or last reset, otherwise it becomes impossible to esimate within what time the number of pages loads counted occurred. Web counter are not trustworthy. A webmaster could start the counter high number, to give the impression that the site is more popular than it actually is.

CHAPTER - 4 BUSINESS APPLICATIONS OF E-COMMERCE

4.1 Introduction

Electronic commerce is the purchasing or selling of goods or services and the transferof funds in any way using electronic communications inter-company and intra company business activities.

4.2 Trade Cycle

A trade cycle is the series of exchanges, between a customer and supplier that take place when a commercial exchange is executed. A general trade cycle consists of:

- Pre-Sales: Finding a supplier and agreeing the terms.
  This phase can be classified in
  - Search
  - Negotiate
    - Execution: Selecting goods and taking delivery.

    This phase can be classified in
  - Order
  - Delivery
    - Settlement: Invoice (if any) and payment.

    This phase can be classified in
  - Invoice
  - Payment
- After- Sales: Following up complaints or providing maintenance.

Nature of the Trade Cycle

For business-to-business transactions the trade cycle typically involves the provision of credit with execution preceding settlement whereas in consumer-to-business these two steps are typically co-incident.

The nature of the trade cycle can indicate the e-Commerce technology most suited to the exchange.

- Commercial transactions that are repeated on a regular basis, such as supermarkets replenishing their shelves, is one category of trade cycle. EDI is the e-Commerce technology appropriate to these exchanges, see Fig 4.1.

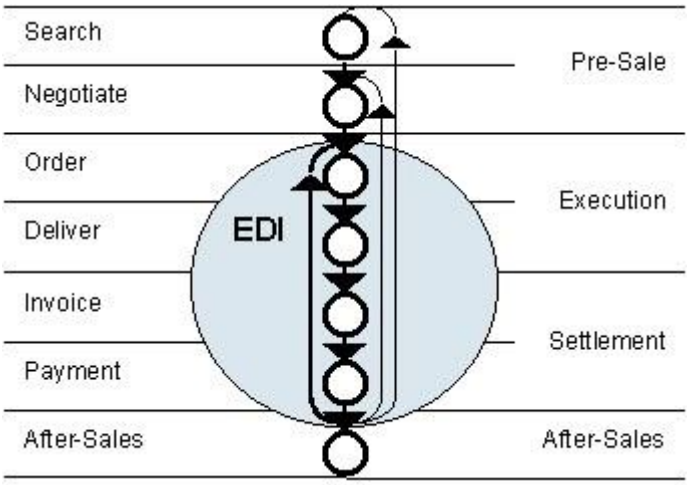


Fig.4.1. EDI Trade Cycle.

- Consumer transactions tend to be once-off (or at least vary each time) and payment is made at the time of the order. Internet e-Commerce is the technology for these exchanges, see Fig.4.2.

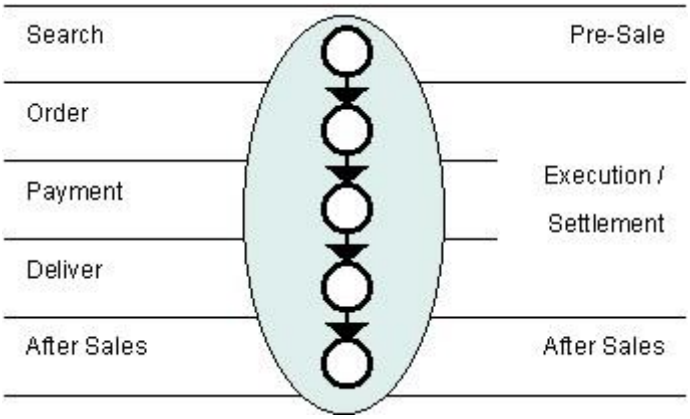


Fig.4.2. Consumer E-Commerce.

- The third generic trade cycle is the non-repeating commercial trade cycle and Internet e-Commerce or an electronic market is the appropriate e-technology.

4.3 Supply Chain

Supply chain is a network of facilities and distribution options that performs the function of procurement of materials from supplier, transformation of these materials into intermediate and finished products (manufacturing) and the distribution of these finished products to customer. This network adds value for customer through the manufacture and delivery of products.

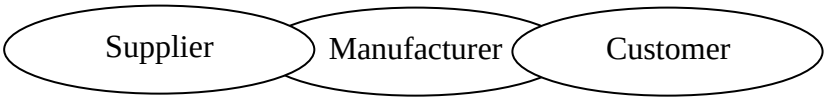


Fig. 4.3. Supply Chain

- The entities of supply chain consist of manufacturers, service providers, distributors & retail outlets.
- Supply chain activities transform raw materials into finished products. The
- primary objective of supply chain management is to fulfill customer demands.
    - Today‘s in business environment, demands are
    - ➢ To provide products & services quicker
    - ➢ With greater added value
    - ➢ To the correct location
    - ➢ With no relevant inventory position
- Customers want more quality, design, innovation, choice, convenience and service, and they also want to spend less money, effort, time & risk.

Supply chain management means transforming a company‘s ―supply chain‖ into an optimally efficient, customer satisfying process, where the effectively of the whole supply chain is more important than the effectively of each individual department.

Porter’s Value Chain Model

In 1985 Michael porter introduces a generic value chain model that comprises a sequence of activities found to be common wide range of firms. Porter identified primary and support activities as shown in the figure 4.4

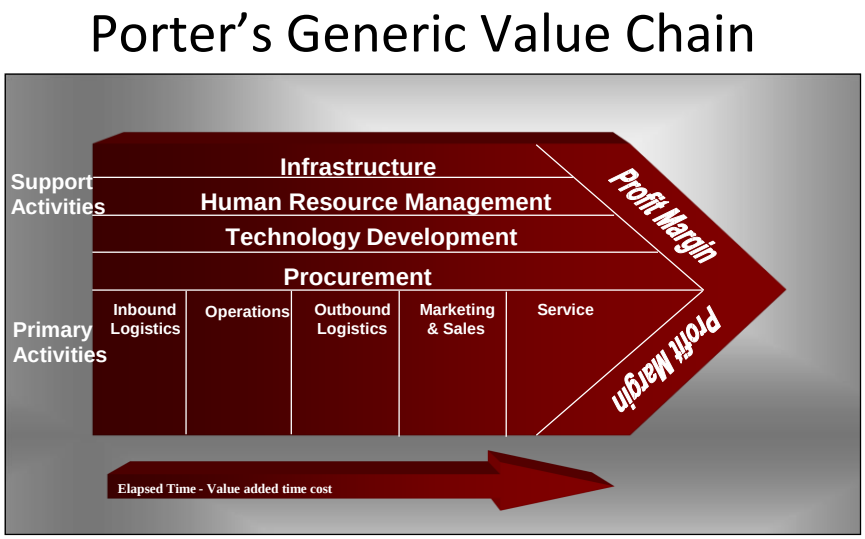


Fig. 4.4. Porter’s value chain model

The primary value chain activities are:

- ❖ Inbound logistics:
  The receiving and warehousing of raw materials and their distribution to manufacturing as they required.
- ❖ Operations:
  The processes of transforming inputs into finished product and services.
- ❖ Outbound logistics:

The warehousing and distribution of finished goods.

- Marketing & sales:
  The identification of customer needs and their generation of sales.
- Service:
  The support of customers after the products services are sold to them.

These primary activities are supported by:

- Infrastructure of the firm:
  Organizational structure, control systems, company culture etc.
- Human resources management:
  Employee recruiting, hiring, training, development and compensation.
- Technology development:
  Technologies to support value creating activities.
- Procurement:
  Purchasing inputs such as materials, supplies, and equipment.

Linked value chains

Value chain activities are not isolated from one another. One value chain activity often affects the cost or performance of other ones. Linkages may exist between primary activities and also between primary and support activities. Interrelationship among business units from the basis for a horizontal strategy. Such business unit interrelationships can be identified by a value chain analysis.

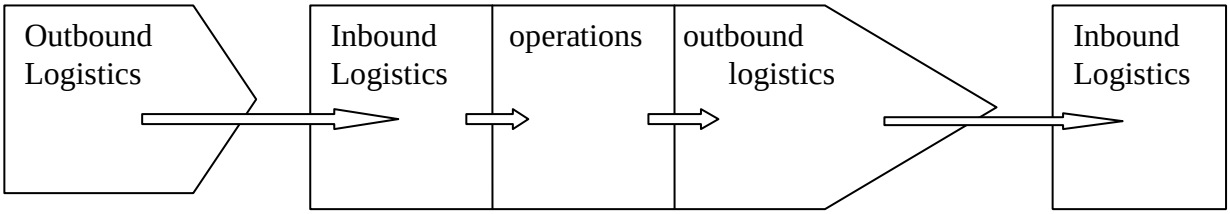


Fig. 4.5. Linked value chain

Inbound logistics ___ from suppliers
Outbound logistics ___ from customers

Role of E-Commerce in Value Chain

- **Intranet** is a secured network of web pages and applications, which can be accessed by anyone within a company firewall.
- **Internet** is a collection of servers and networks which allows users access to information and application outside of the company firewall.
- **Extranet** is a collaborative network that uses internet technology to link business with their suppliers, customers, or partners that share common goals.
- **E-Commerce** is buying and selling electronically.
- **E-Business** is using the capabilities of internet technology to conduct business electronically.

E-Commerce enhances value chain by providing:

- Electronic value chain:

  E-commerce enhances business by supporting
  - Reduce time frame
  - Changed cost structures Re-engineered
- value chain:

  E-commerce enhances business by supporting
  - Just in time manufacturer
  - Quick response supply
  - Efficient document processing
- Competitive advantage:

  E-commerce supports a company for gaining competitive advantage.

E-business provides various strategies for supply chain. These are

- E-Procurement:

  E-Procurement provides cross enterprise system to system integration, electronic catalogs, online buying and selling. Advantages of e-procurement are Enhances
  - efficiency.
  - Reduce cost/cycle time.
  - Helps in contract compliance and customer reach.
- E-Collaboration:

  E-Collaboration provides cross enterprise technology / design interaction. Advantages of e-collaboration are
  - Design cycle time
  - Design synergy, reuse
  - Revenue
- Integrated Planning/ Manufacturing:

  Integrated Planning / Manufacturing provide cross enterprise planning / execution, system to system integration and outsourced manufacturing visibility. Advantages of

  Integrated Planning /
  - Manufacturing are Lead time,
  - margin.
  - Accuracy/flexibility.
  - Inventory levels.
- On time delivery.

  Integrated delivery:

  Integrated delivery provide cross enterprise logistics management / consignment visibility. Advantages of Integrated delivery are
  - Logistics cycle time.
  - Reduced cost.
  - Lead time.

- Online marketing:

On line marketing provides product boundary extension, new products/ services creation, new markets/ channels creation. Advantages of online marketing are Market segment share. Customer reach.

4.4 E-Procurement

Electronic procurement is the use of electronic tools & system. To increase efficiency & reduce cost during each stage of the purchasing process.

E-procurement can be divided into two parts:-

❖**Direct material procurement:-**

Direct material procurement in which raw materials or components needed for production are procured from supply chain partner.

As direct materials are needed for the production process, they require greater scrutiny before ordering, organization need to focus on different issue like the integration of suppliers, methods for integrity etc. Usually these items should be ordered in appropriate quantities is inventory of these can add further cost.

❖**Indirect materials procurement**

Materials that are indirectly used are procured (like office supplies, maintenance related materials and operation related supplies).

Indirect materials usually have law value, are not critical to the main, production process & are ordered in high volume.

In an organization, large no. of people orders these items. By ordering these items online a company can save valuable amount of money and other resources.

The three ways in which these materials can be procured online are:-

- Seller side solutions
- Buyer side solutions
- Third-party solution

Seller side E-procurement solution:-

The supplier‘s technological infrastructure, ability to integrate with different technological platform and ability to cut cost & improve products.

Several supplier of a single product having coming together to form vertical portal.

Vertical portal are commonly seen in industries like still, paper and chemical where fragmented market and price variation make it difficult for buyer to make a purchasing decision.

Buyer side E-procurement solution:-

It should be user friendly & help employees place order and purchase goods from their desktop with ease.

It should provide a list of preferred supplier for each product and help reduced non compliance with the organization business rule for purchasing.

Organizations are moving from the business -to-supplier model to a trading community model .In this model several suppliers of particular product category come together to form a vertical portal.

Indiamart.com provides on such kind of catalog. These kinds of portals represent a comprehensive catalog, which consists of the product details of all the participating suppliers.

The buyers can access the catalog, compare product features & prices, select a supplier & place the order.

Since price and product differentiation play an important role in influencing the buyers purchasing decision, the suppliers participating in this model should continuously improve their product and cut costs.

4.5 Implementing E-Procurement

Organizations want their E-procurement system to offer maximum benefit at the lowest cost. The general expectations of the organization form E-procurement solution are

- Quick & positive result with minimum risks
- Leveraging of the hue buying potential of the organization to negotiate favorable contracts from supplier.
- Limiting the no. of supplier by choosing only efficient company as preferred supplier.
- Adopting best practices in procurement.

E-procurement solution that needs the above expectation.

The chief procurement officer (CPO) should ensure that the solution provider understands the exact requirement of the organization .To obtain the desired E-procurement for the organization the steps are:-

- Establish E-procurement chain goal:-

  Implementing an E-procurement is to defined the objective of e-procurement .The objective of e-procurement are to automate the purchasing process cut cost, obtain accurate purchase report and eliminate unauthorized purchases.

- Construct a procurement audit:-

  The organization should evaluate its existing process & determine whether it can be written or require some modification.

  If all the purchasing info is not available at a single location or if it is not accurate or easily accessible the procurement processes need to be modified.

  The most widely used technique for systematic measurement of e-procurement effectiveness is return on asset (ROA).

ROA= {(Revenues –Expanses)/assets} * 100

  The e-procurement system can increase ROA by increasing revenues, decreasing expenses or minimizing investments in assets.

- Develop supplier integration matrix:-

  An organization cannot maintain the same kind of relationship with all its suppliers.

It has to formulate it relationship strategy depending on the contribution of each supplier to the success of the company.

Some suppliers produce critical components to the business and maintaining long-term relationships with is crucial to the organizations success.

- Select an e-procurement application:-

  The selection of e-procurement application is critical and should be guided by factors like application should improve current procurement process, application should leverage the investments already made by the organization in ERP /SAP system and should be flexible enough to accommodate new procurement practices.

- Focus on integration

Each area of operating resource management (ORM) and the requirement of the employees buyer and supplier should be considered in the design of the e-procurement application.

- Educate the staff

Educating the employee in another imp factor for implementing a new eprocurement system .it is the employee who will use the system and help the organisation to achieve the desired improvement in the procurement chain and cost. In the employee oppose the system because of its complexity of other fear like lay of then the eprocurement system will fail. Despite the advance technology used and huge investment.

E-procurement tools relate to two aspects of procurement:

- Sourcing activity
- Transactional purchasing

Sourcing activity (E-sourcing)

The E-sourcing tools described can help buyers establish optimum contracts with suppliers and manage them effectively. The tools include supplier database and electronics tendering tools, evaluation, collaboration and negotiation tools. Also included are E-auction tools and those tools which support contract management activity.

Transactional purchasing (E-purchasing):-

The e-purchasing tools can help procurement professionals and end users where more efficient process and more accurate order details. The two main aims of

- Minimizing control
- Process efficiency is the function of E-purchasing tools such as purchase –to-pay system, purchasing cards and electronic invoicing system.

The government procurement cart (GPC) is an established and widely accepted programme. Implementing the GPC will provide most organisations with immediate process efficiency gains and the capability to better meet prompt payment targets.

Purchasing cards:-

Purchasing cards are similarly in principle to smart cards used by consumers but with extra features which make them more suitable for b2b purchasing.

Those can include:-

- Control such as restricting or due to particular commodity
- areas. Individual transaction values and Monthly expenditure
- co nits.

Implementing p-cards:-Card

holders (users)

p-cards should be distributed to anyone in the organisation who needs to re-question low value goods same series .

Functionality:-

P-cards enables each cards holder to be allocated a spend limit per transaction and a total spend limit per month.

The GPC and some other p-cards programmes also enable spend to require by blocking spend categories for particular users.

Individual transaction data is captured by the supplier at time of sale and transmitted to the issuing bank which provides the card programme.

A monthly consolidated statement is provided in paper format or electronically to the purchasing organisation for approval and payment.

Benefit of p-cards:-

- Prompt payment discounts deduce the amount paid for goods and services.
- Granting prompt payment is a significant benefit to supplier, particularly small and medium sized enterprise as it generates cash flow increased compliance with contracts.

E-auction:

E-auction can be based on price alone or can be weighted to account for other criteria. such as quality ,delivery or service levels.

Electronic reverse auctions (ERA) frame world:

Each of the e-auction service providers on the frame. Work offers public sector organisation assistance with:-assessment suitability of forth coming contracts to the e-auction process advice and guidance on strategy & supplier training & test e-auction events.

E-auction benefits:

- Improved preparation & planning for the tendering process.
- Opportunity for suppliers to submit revised bids for a contract.
- Increased market knowledge for buyers & suppliers. Suppliers particularly benefit from increased awareness of competitor pricing.
- Provides a more level/playing field for suppliers improve quality of service.

Implementing e-auctions:

E-auctions do not replace tendering: they are a part of it and provide cost-effective, fast and transparent conclusions not full tendering process.

Auctions may be based on securing the lowest price or on most economically advantageous bid (price, Payment terms, supply, and schedules).

Only those suppliers who have successfully pre-qualified (i.e. they have satisfied all tendering criteria such as quality process, financial stability and environmental policies) should be invited to participate. Identifying purchases suitable for e-auctions.

Advantages of e-procurement

- Price savings
- Process cost reduction (head count)
- Reductions in cycle times (days/weeks)
- Consequent reductions in inventory holdings (value/stock turnover)

Disadvantages of e-procurement

- Bandwidth problems
- Securityissues
- Accessibility
- Acceptance

4.6 Competitive Advantage

When two or more firms compete within the same market, one firm possesses a competitive advantage over its rivals when it earns a persistently higher rate of profit.

Michael porter identified two basic types of competitive advantage:

- Cost advantage
- Differentiation advantage

Cost Leadership Strategy

The goal of cost leadership strategy is to offer products or services at the lowest cost in the industry. The challenge of this strategy is to earn a suitableprofitfor the company, rather

than operating at a loss and draining profitability from all market players. Companies such asWalmartsucceed with this strategy by featuring low prices on key items on which customers are price-aware, while selling other merchandise at less aggressive discounts. Products are to be created at the lowest cost in the industry. An example is to use space in stores for sales and not for storing excess product.

Differentiation Strategy

The goal of differentiation strategy is to provide a variety of products, services, or features to consumers that competitors are not yet offering or are unable to offer. This gives a direct advantage to the company which is able to provide a unique product or service that none of its competitors is able to offer. An example is Dell which launched masscustomizations on computers to fit consumers' needs. This allows the company to make its first product to be the star of its sales.

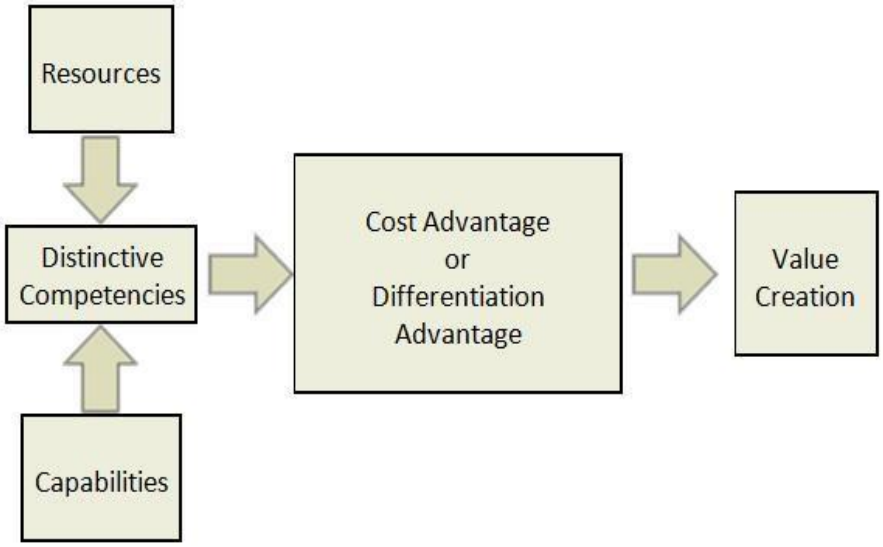


Fig. 4.6. Model of competitive advantage

Resources and capability:-

According to the resource-based view, in order to develop a competitive advantage the firm must have resources and capabilities that are superior to those of its competitors without this superiority, the competitors simply could replicate what the firm was doing and any advantage quickly would disappear.

Resources are the firm-specific assets useful for creating a cost or differentiation advantage and that few competitors can acquire easily. Examples of such resources are:-

- Patents and trademarks
- Proprietary know-how
- Installed customer base
- Reputation of the firm
- Brand equity

Capabilities refer to the firm‘s ability to utilize its sources effectively. Example of a capability is the ability to bring a product to market faster than competitors. Such capabilities

are embedded in the routines of the organization and are not easily documented as procedures and thus are difficult for competitors to replicate

Porter's Five Forces Model

Porter identified five factors that act together to determine the nature of competition within an industry, potential competitors, suppliers, buyers. These are the:

- Threat of new entrants to a market
- Bargaining power of suppliers
- Bargaining power of customers (—buyers‖)
- Threat of substitute products
- Degree of competitive rivalry

The five forces are:

- **Supplier power.** An assessment of how easy it is for suppliers to drive up prices. This is driven by the: number of suppliers of each essential input; uniqueness of their product or service; relative size and strength of the supplier; and cost of switching from one supplier to another.
- **Buyer power.** An assessment of how easy it is for buyers to drive prices down. This is driven by the: number of buyers in the market; importance of each individual buyer to the organisation; and cost to the buyer of switching from one supplier to another. If a business has just a few powerful buyers, they are often able to dictate terms.
- **Competitive rivalry**. The main driver is the number and capability of competitors in the market. Many competitors, offering undifferentiated products and services, will reduce market attractiveness.
- **Threat of substitution.** Where close substitute products exist in a market, it increases the likelihood of customers switching to alternatives in response to price increases. This reduces both the power of suppliers and the attractiveness of the market.
- **Threat of new entry.** Profitable markets attract new entrants, which erodes profitability. Unless incumbents have strong and durable barriers to entry, for example, patents, economies of scale, capital requirements or government policies, then profitability will decline to a competitive rate.

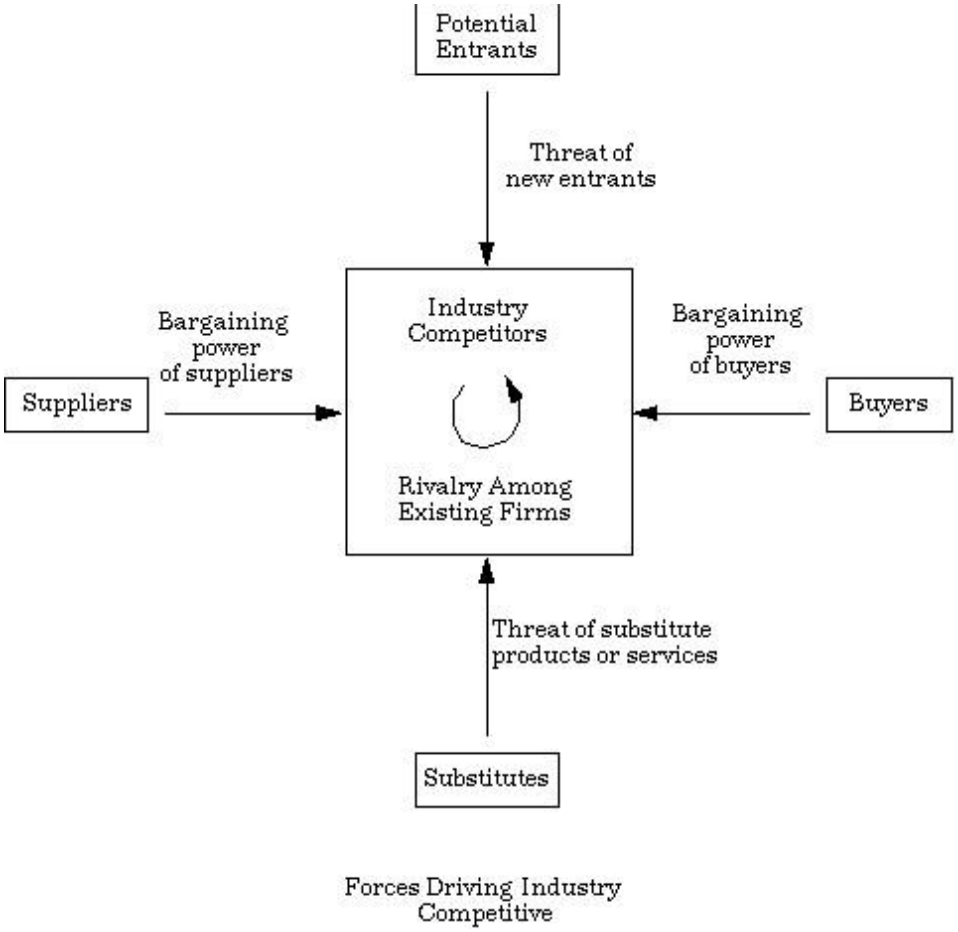


Fig. 4.7. Porter's model for competitive forces

4.7 E-Commerce Application in Manufacturing

- Manufacturing can be defined as the process of collecting and then converting raw materials into finished, qualitative goods or products for the consumers.
- Manufacturing requires a web of various components, contracts personnel etc working intricately together and in order to produce goods or services.
- Manufacturing requires components, assemblies, transportation, storages, paper works, etc.
- E-Commerce applied to the supply chain management process helps in reducing the overall costs drastically and improves quality and efficiency by automating most of the supply chain.
    - E-commerce can enhance manufacturing process by:
        - Enhancing efficiency.
        - Reducing cost/cycle time.
        - Providing accuracy and flexibility.
        - Supporting inventory levels.

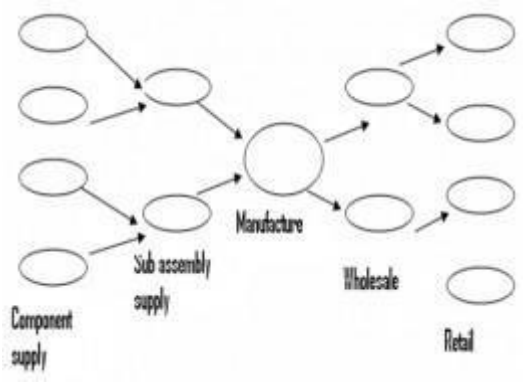


Fig. 4.8. Manufacturing (supply chain)

4.8 E-Commerce Application in Wholesale

- Selling goods or products in large quantities to anyone other than the consumers, for example the retailers, industrial/ commercial or other business users or even distributors are known as wholesalers.

- Physical assembling, sorting & grading goods in large lots, breaking bulk, repacking & redistributing in smaller lots is all a part wholesale.

Problems faced by the traditional system of wholesale:

- The local wholesalers could not compete with the foreign wholesale enterprises who had acquired highly advanced management and operational skills over due time.

- The wholesale sector was characterized for its high input and low output.

- Wholesale operating costs which included staffing, setting up and acquiring land for local warehouses, establishing distribution centers, etc were extremely high.

Role of E-Commerce in wholesale:

- Reduced operating costs, access to accurate and correct information on time & quick responses helps in qualitative and efficient decision making.
- Ability of doing global marketing in less time and cheaper
- Gaining and catching up to the competitive edge held by foreign wholesalers such as MNC‘s
- Offers a wide and extensive range of information, intermediary and business services.

4.9 E-Commerce Application in Retail

- Selling of goods and services to the consumers for their personal consumption and use is known as **retailing.** For example Ebay.com, departmental stores, then services like dentists, doctors, hotels, etc.

- Retailers provide a link between the consumers and the manufacturers and add value to the product and service by making their sales easier.

- Retailers answer any queries that you may have they display and demonstrate products to the consumers before selling it to them. This makes the services by retailers less risky and more fun to buy products.
- They even provide extra services from personal shopping to gift wrapping and home delivery.

Role of E-Commerce in Retailing:

- The Internet has made retailing an exciting and challenging field in recent days with various companies hosting their stores online via the internet.
- People can now sit at their computers, open the website they desire to do so and browse their catalogues put up by the company (retailer), choose their product and either pay for it online itself or on delivery. You don't need to step out to your room to make a purchase nowadays.
- Having your store online helps drastically in cost cutting as companies don't need to purchase stores, they can cut down on staff, provide services to a much wider audience, etc

4.10 E-Commerce Application in Service Sector

- One of the three main industrial categories of a developed economy is the service sector.
- It involves basically the provision of all services such as distribution and sales of goods to other businesses and consumers such as pest control, entertainment and even services such as transportation.
- It also includes the public utilities and the soft parts of the economy such as insurance, banking, education, etc.
- The service sector focuses mainly on people to people services.

Issues Faced by the Service Sector:

- Since services are intangible, it‘s extremely difficult to make customer understand and aware about their benefits.
- Quality of services depends solely on the quality of the individual providing the services.
- There's no special technology or anything like in manufacturing to attract people.

Role of E-Commerce in the Service Sector:

- E-Commerce helps in improving and increasing the speed of transactions, reduces management expenditure, and increases efficiency and increases competitiveness.
- Helps the insurance, banking and mainly all the financial sectors, real estate, telecommunications, tourism, logistics, and postal services.
- E-Commerce also helps services gain a competitive advantage by providing strategies for differentiation, cost leadership and customer satisfaction.

CHAPTER - 5
E-COMMERCE IN TECHNOLOGY

5.1 Introduction

E-commerce brings new form s of markets to the consumer and to industry, though the connectivity provided by the internet. The web is responsible for new kinds of markets.

5.2 IT infrastructure

Introduction to Information technology

Information technology refers to the creation, gathering, processing, storage, and delivery of information and the processes and devices that make all this possible.

Characteristics of IT infrastructure

1. Efficient support for the exchange of information within the organization and with other organizations.
2. Reliable availability of information processing capabilities whenever and wherever they are needed.
3. Preservation of the integrity and confidentiality of information maintained by the organization.
4. Sufficient flexibility to allow the timely and efficient addition of new information management capabilities and modifications of established capabilities.
5. Consistency with a coherent set of technical and managerial standards for the employment of information technology.

Elements of IT Infrastructure

1. **Application system:** The applications that an organization purchases and/or develops to achieve personal productivity and program support benefits.
2. **Architecture**: The guidelines or blueprints that an organization follows in designing, acquiring, and implementing information technology solutions. Organizationally approved definitions, specifications, and standards are the primary components in organization‘s information technology architecture.
3. **Communications:** Local area and wide area network components, including linkages with other organizations.
4. **Equipment:** An organization‘s hardware platforms and components ranging from individual personal computers to mainframes and associated peripherals.
5. **Facilities**: The electrical, ventilation, fire suppression, physical security, wiring, and other components required to support an organization‘s information technology capability, including the physical structure itself.
6. **Funding:** Current and projected funding for information technology planning, acquisition, development, and operations activities.
7. **Partnerships:** Relationships with other public and private sector organizations that support and enable the organization‘s pursuit and use of information technology.

8. **People:** An organization‘s technical staff, user community groups, and executive steering and oversight committees that are charged with information technology planning, approval, development, management, operations , and security responsibilities.
9. **Plans:** Detailed designs or methods for aligning information technology activities with organization business strategies and accomplishing business objectives. Typical organization information technology plans include strategic, risk management and operational recovery.
10. **Policies:** The rules, conventions, and protocols adopted by the organizations to govern the pursuit and use of information technology.
11. **Processes and procedures:** The defined steps for planning, approving, acquiring, developing, operating, maintaining, enhancing, and using information technology within the organization.
12. **Service definitions:** The types of service provided, accepted service levels, and service delivery time frames established for an organization‘s information technology support organization.
13. **Software**: The set of operating system , utility, communication, user interface , and management programmers that enables user to operate and control computers and develop application systems.
14. The infrastructure includes elements owned by the organization and available under contract or through inters organization agreement. For agencies that employ the services of a consolidated data centre, for example, the required data centre resources are considered part of the organization‘s infrastructure.
15. **Reengineering the business process:** The search for , and implementation of, radical change in business processes that result in dramatic efficiencies, reductions in turnaround time ,Improvement in quality, or improvement in customer service.
16. **Strategic planning process for information technology:**The process of aligning organization plans for, and uses of, information technology with the organization‘s business strategies.

5.3 Internet

Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Characteristics of Internet:

- **Interoperable: I**nteroperable means that the standards allow communication across networks. This does not limit the access of information to a proprietary site, location, machine or band name.
- **Packet switched: C**onnection are not fixed from point to point for the duration of the transmission. A telephone call is circuit switched-which means a dedicated path is established to transmit your entire conversation. When data is sent packet switched

over the internet-it transmits a small part of the data, verifies it is correct then sends more information toward the destination. Packet switched networks do not require all of the information to be delivered through the same path. By not dedicating the path for the duration of the connection, this method allows more connections to be sending information across the same space or allows for sharing resources.

- **Data network:** A network that carries data information (digital- computer) instead of voice information (analog-telephone). There are many instances where these —definition —of data and voice are starting to overlap. Computers connecting to regular phone lines are technically carrying data over a voice line and in some progressive parts of the country digital phone lines are starting to make appearances.

History of Internet

❖**1960's**

1969- The department of defence advanced research projects organization (ARPA) creates an experiment network called ARPANET. This network provides a test-bed for emerging network technologies. ARPANET continued to expand, connecting many more sites throughout the 1970's and 1980's.

❖**1970's**

Networking tools are developed in the 1970's such as

1972- The national centre for supercomputing applications (NCSA) develops the telnet application for remote login, making it easier to connect to a remote computer.

1973- FTP (file transfer protocol) is introduced, standardizing the transfer of files between networked computers.

❖**1980's**

TCP/IP suite of networking protocols, or rules, becomes the only set of protocols used on the ARPANET. To keep military and non-military network sites separates, the ARPANET splits into two networks: ARPANET and MILNET.

1982-1983:-

The first desktop computers begin to appear. Many are equipped with an operating system called Berkeley UNIX which includes networking software.

1985-86:-

The national science foundation(NSF) connects the nation's six supercomputing centers together. This network is called the NSFNET, or NSFNET backbone. **1987:-** the NSF awards a grant to merit network, inc to operate and manage future development of the NSFNET backbone.

1989- the backbone network is upgraded to —TI‖ which means that it is able to transmit data at speeds of 1.5 millions bits of data per second, or about 50 pages of text per second.

❖**1990's**

1990- the ARPANET is dissolved.

1991- gopher is developed at the university of Minnesota. Gopher provides a hierarchical, menu-based method for providing and locating information on the internet.

1993- European laboratory for particle physics in Switzerland(CERN) releases the world wide web(WWW), developed by Tim burners-lee. The WWW uses hypertext transfer protocol(HTTP) and hypertext links, changing the way information can be organized, 1993- the NSFNET backbone network is upgraded to ―T3‖which means that it is able to transmit data at speeds of 45 millions bits of data per second, of about 1400 pages of text per second.

1993-1994- the graphical web browser mosaic and Netscape navigator are introduced and spread through the internet community.

1995- the NSFNET back bone is replaced by a new network architecture, called VBNS(very high speed backbone network system) that utilizes network service providers, regional networks and network access points(NAPs).

How Internet Works

To visit any website.

- First you enter the address of URL of the website in your web browser.
- Then your browser requests the web page from the web server that hosts the site.
- Then server sends the data over the internet to your computer.
- Then your web browser interprets the data, displaying it on your computer screen.

To access the web we need a web browser, such as Netscape navigator or Microsoft internet explorer. Web pages are written in a computer language called HTML

WWW:-

The World Wide Web, also referred to as the WWW and ―the web,‖ is the universe of information available via hypertext transfer protocol (HTTP). The World Wide Web and HTTP:

- Allow you to create ―links‖ from one piece of information to
- another; Can incorporate references to sounds, graphics, and movies, etc;
- ―Understand‖ other internet protocols, such as ftp, gopher, and telnet.

The web presents information as a series of ―document,‖ often referred to as web pages that are prepared using the **Hypertext Markup Language (HTML).**

Using HTML, the document's author can specially code sections of the document to ―point‖ to other information resources. These specially coded sections are referred to as **hypertext links**. Users viewing the web page can select the hypertextlinks and retrieve or connect to the information resources that the link points to.Hypertext ―links‖ can lead to other documents, sounds, images, databases (like library catalogs), e-mail addresses, etc.

The World Wide Web is non-linear:

Non-linear means you do not have to follow a hierarchical path to information resources.

- You can jump from one link (resource) to another:
- You can directly to a resource if you know the uniform resource locator (**URL**)
- You can even jump to specific parts of a document.

Because the web is not hierarchical and can handle graphics, it offers a great deal of flexibility in the way information resource can be organized, presented, and described.

Advantages of WWW:

The webs are flexibility in organizing and presenting information, it‘s non- hierarchical easy-to-navigate structure, its ability to handle and ―understand‖ many different file formats and internet protocols, and its overall ease of use.

Domain Name

A Domainname is a way to identify and locate computers connected to the internet. No two organizations can have the same domain name.

A Domainname always contains two or more components separated by periods, called ―dots‖.

Once a Domainname has been established, ―sub domain‖ can be created within the domain.

The structure for this is:

Hostname.subdomain.second-level domain.top-level domain

For ex- a,Indian.yahoo.com describes a single host computer named a, in the India office of the yahoo company.

The top-level portion of a domain name describes the type of organization holding that name. The major categories for top-level domains are:

- COM-commercial entities
- EDU-four year colleges and universities
- NET- organization directly involved in internet operations, such as network providers and network information centers.
- ORG-miscellaneous organization that don‘t fit any other category, such as nonprofit groups
- GOV-government entities
- MIL-united states military
- COUNTRY CODE-a two letter abbreviation for a particular country. For example, ―IN‖For India or ―UK‖ forunited kingdom.

Client-Server

The client-server describes the relationship between the client and how it makes a service request to the server, and how the server can accept these requests, process them, and return the requested information to the client. The interaction between client and server is often described usingsequence diagrams.

Client

In client –server architecture, client is a computer or process that request from a server. It is often an application that uses a graphical user interface. Each instance of the client software can send requests to a server.

Types of Client

Clients are classified in different types

- Fat Clients: A fat client is also known as thick client or rich client. It is a client that performs the bulk of any data processing operations itself, and does not necessarily rely on the server. The fat client is in the form of a PC or laptop.
- Thin clients: A thin client is a minimal sort of client. Thin client uses the resources of the host computer. A thin client_s job is generally just to graphically display picture provided by an application server, which platforms the bulk of any required data processing.
- Hybrid clients: A hybrid client is also called a smart client. it is a mixture of the fat and thin client. Similar to fat client, it is processed locally, but rely on the server for the storage. This relatively new approach offers features from both the fat client and the thin client.

Characteristics of Client

- Always initiates requests toservers.
- Waits for replies.
- Receives replies.
- Usually connects to a small number ofserversat one time.
- Usually interacts directly with end-users using anyuser interfacesuch asgraphical user interface.

Server

In client –server architecture, server is simply a computer that is running software that enables it to serve specific requests from computers called clients.

Characteristics of Server

- Always wait for a request from one of the clients.
- Serveclientsrequests then replies with requested data to the clients.
- Aservermay communicate with other servers in order to serve a client request.
- A server is a source which sends request to client to get needed data of users.

Basic server software

- **Network operating system**:

  There are many different operating systems for servers just like there are many different operating systems for desktop computers. Windows server (NT, 2000, 2003), Linux, Novell Netware are the main operating systems competitors.

  A network operating system will have many build-in features including such as file serving, print serving, back up and security. Some NOS also include a web server or mail server.

- **Server application:**

  Server can be designed for nearly every purpose imaginable, from fax server to remote acess servers. Every application will have specific server requirements and will be typically designed to run on either Windows NT/ 2000, Linux or Netware. Many servers often run multiple applications to serve a variety of needs.

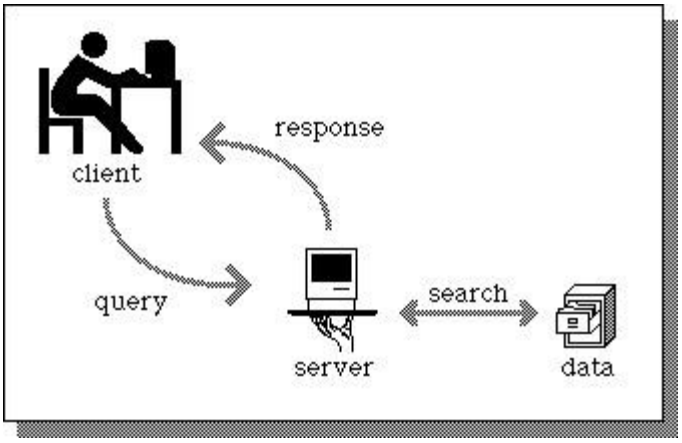


Fig. 5.1. Request &response in client/server

TCP/IP

Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite. Each layer of the TCP/IP has a particular function to perform and each layer is completely separate from the layer(s) next to it. The communication process that takes place, at its simplest between two computers, is that the data moves from layer 4 to 3 to 2 then to 1 and the information sent arrives at the second system and moves from 1 to 2 to 3 and then finally to layer 4.. The 4 layers are as follows:-

1. Application layer
2. Transport layer

3. Network layer
4. Data link layer

Application layer

This is the top layer of TCP/IP protocol suite. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers.

At each layer there are certain protocol options to carry out the task designated to that particular layer. So, application layer also has various protocols that applications use to communicate with the second layer, the transport layer. Some of the popular application layer protocols are :

- HTTP (Hypertext transfer protocol)
- FTP (File transfer protocol)
- SMTP (Simple mail transfer protocol)
- SNMP (Simple network management protocol) etc

Transport Layer

This layer provides backbone to data flow between two hosts. This layer receives data from the application layer above it. There are many protocols that work at this layer but the two most commonly used protocols at transport layer are TCP and UDP.

TCP is used where a reliable connection is required while UDP is used in case of unreliable connections.

Network Layer

This layer is also known as Internet layer. The main purpose of this layer is to organize or handle the movement of data on network. By movement of data, we generally mean routing of data over the network. The main protocol used at this layer is IP. While ICMP (used by popular ‗ping‘ command) and IGMP are also used at this layer.

Data Link Layer

This layer is also known as network interface layer. This layer normally consists of device drivers in the OS and the network interface card attached to the system. Both the device drivers and the network interface card take care of the communication details with the media being used to transfer the data over the network. In most of the cases, this media is in the form of cables. Some of the famous protocols that are used at this layer include ARP(Address resolution protocol), PPP(Point to point protocol) etc.

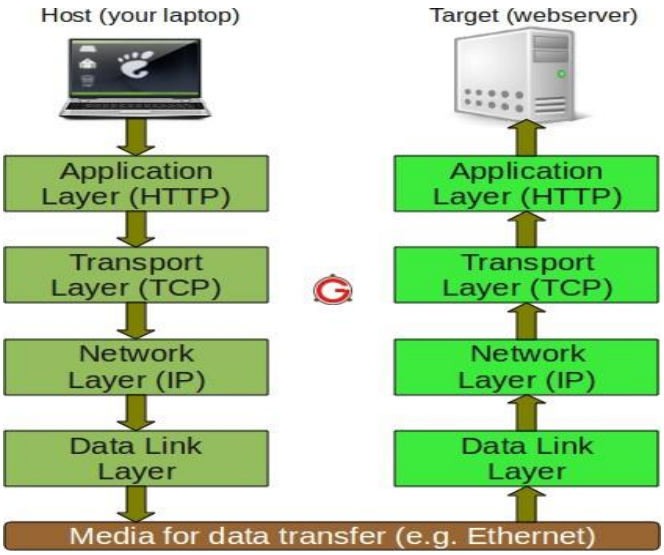


Fig. 5.2. TCP/IP layering model

Web Server

Web servers arecomputersthat deliver (*serves up*)Webpages. Every Web server has anIPaddressand possibly adomainname. For example, if you enter theURL*http://www.pcwebopedia.com/index.html* in yourbrowser, this sends a request to the Web server whose domain name is*pcwebopedia.com*. The server then fetches the page named*index.html* and sends it to your browser.

Any computer can be turned into a Web server by installing server softwareand connecting the machine to theInternet. There are many Web server software applications, including public domain software from NCSA and Apache, and commercial packages from Microsoft,Netscapeand others.

HTTP & FTP

HTTP

H*yper* **T***ext***T***ransfer***P***rotocol***,** HTTP is the underlyingprotocolused by theWorldWideWeb. HTTP defines how messages are formatted and transmitted, and what actionsWebserversandbrowsersshould take in response to various commands. For example, when you enter aURLin your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requestedWebpage.

FTP

F*ile***T***ransfer***P***rotocol*, theprotocolfor exchangingfilesover theInternet. FTP works in the same way asHTTPfor transferring Web pages from aserverto a user's browser and SMTPfor transferringelectronicmailacross the Internet in that, like these technologies, FTP uses the Internet'sTCP/IPprotocols to enable data transfer.

FTP is most commonly used todownloada file from a server using the Internet or touploada file to a server (e.g., uploading a Web page file to a server).

5.4 Middleware

Middleware is the layer of software between client and server processes that deliver the extra functionality.

While network protocols such as TCP/IP enable the exchange of data between client and server, more functionality required for communication in internet i.e. between client and server. To support additional services a concept known as middleware.

Some middleware services are:

- Remote data access (RDA): It provides SQL access to server based DBMS.
- Remote Procedure call (RPC): It provides invocation of remote procedures.
- Message oriented middleware: It provides, store and forward message queuing between application processes.
- Object request brokers (ORB): it provides invocation of remote objects by simply sending a message to it.
- Distributed Transaction Processing: It provides invocation of remote transactions with transactional execution.

5.5 Intranet

Intranet is defined as private network of computers within an organization with its own server and firewall. Intranet can define as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Every computer in internet is identified by a unique IP address.
- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.

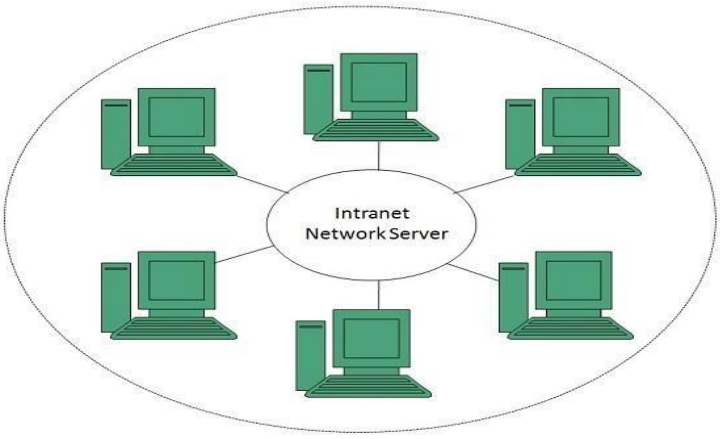


Fig. 5.3. Intranet

Benefits

Intranet is very efficient and reliable network system for any organization. It is beneficial in every aspect such as collaboration, cost-effectiveness, security, productivity and much more.

- Communication

Intranet offers easy and cheap communication within an organization. Employees can communicate using chat, e-mail or blogs.

- Time Saving

Information on Intranet is shared in real time.

- Collaboration

Information is distributed among the employees as according to requirement and it can be accessed by the authorized users, resulting in enhanced teamwork.

- Platform Independency

Intranet can connect computers and other devices with different architecture.

- Cost Effective

Employees can see the data and other documents using browser rather than printing them and distributing duplicate copies among the employees, which certainly decreases the cost.

- Workforce Productivity

Data is available at every time and can be accessed using company workstation. This helps the employees work faster.

- Business Management

It is also possible to deploy applications that support business operations.

- Security

Since information shared on intranet can only be accessed within an organization, therefore there is almost no chance of being theft.

- Specific Users

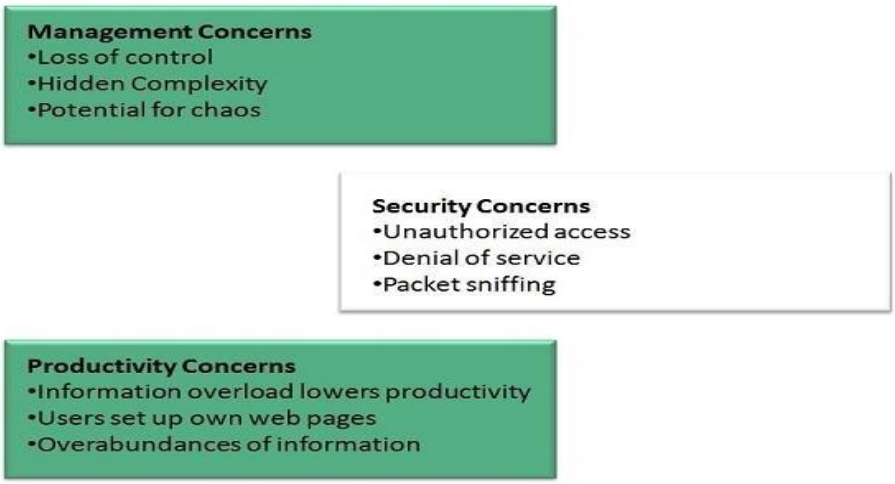
Intranet targets only specific users within an organization therefore, once can exactly know whom he is interacting.

- Immediate Updates

Any changes made to information are reflected immediately to all the users.

ISSUES

Apart from several benefits of Intranet, there also exist some issues.. These issues are shown in the following diagram:



Applications

Intranet applications are same as that of Internet applications. Intranet applications are also accessed through a web browser. The only difference is that, Intranet applications reside on local server while Internet applications reside on remote server. Some of these applications are:

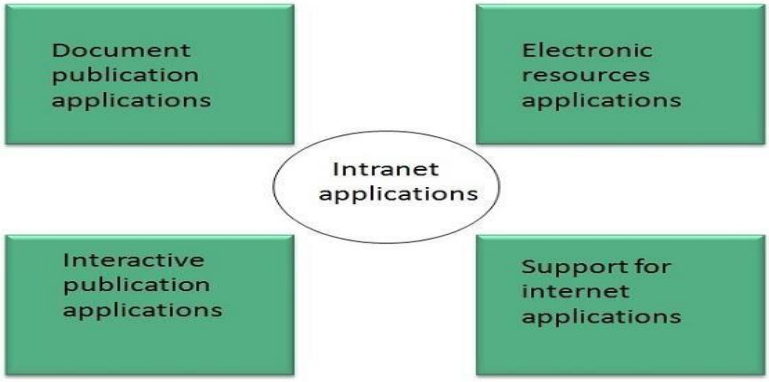


Fig.5.4. Application of intranet

- Document publication applications

Document publication applications allow publishing documents such as manuals, software guide, employee profits etc without use of paper.

- Electronic resources applications

It offers electronic resources such as software applications, templates and tools, to be shared across the network.

- Interactive Communication applications

Like on internet, we have e-mail and chat like applications for Intranet, hence offering an interactive communication among employees.

- Support for Internet Applications

Intranet offers an environment to deploy and test applications before placing them on Internet.

Internet vs. Intranet

Apart from similarities there are some differences between the two. Following are the differences between Internet and Intranet:

Intranet	Internet
Localized Network.	Worldwide Network
Doesn't have access to Intranet	Have access to Internet.
More Expensive	Less Expensive
More Safe	Less Safe
More Reliability	Less Reliability

5.6 Extranet

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.

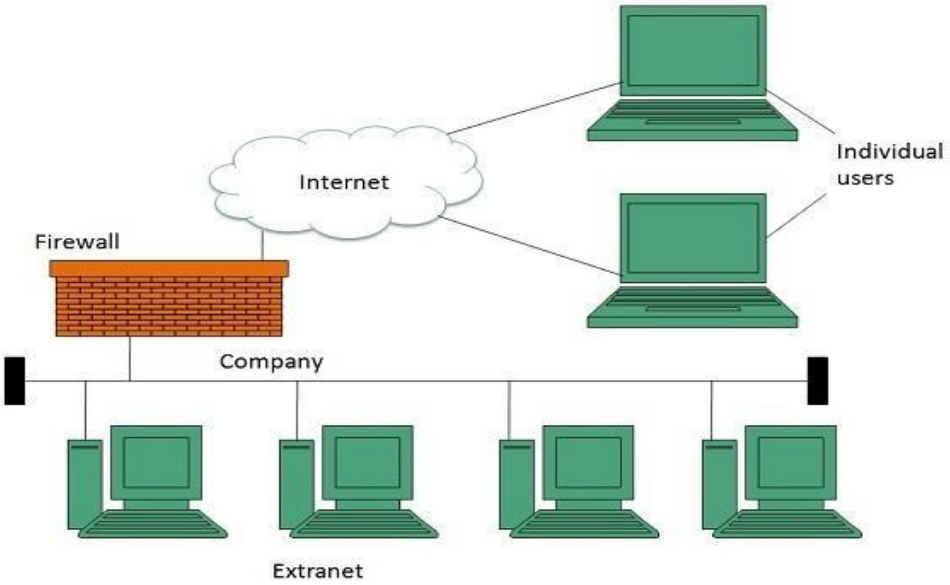


Fig. 5.5. Extranet

Implementation

Extranet is implemented as a Virtual Private Networks (VPN) because it uses internet to connect to corporate organization and there is always a threat to information security. VPN offers a secure network in public infrastructure (Internet).

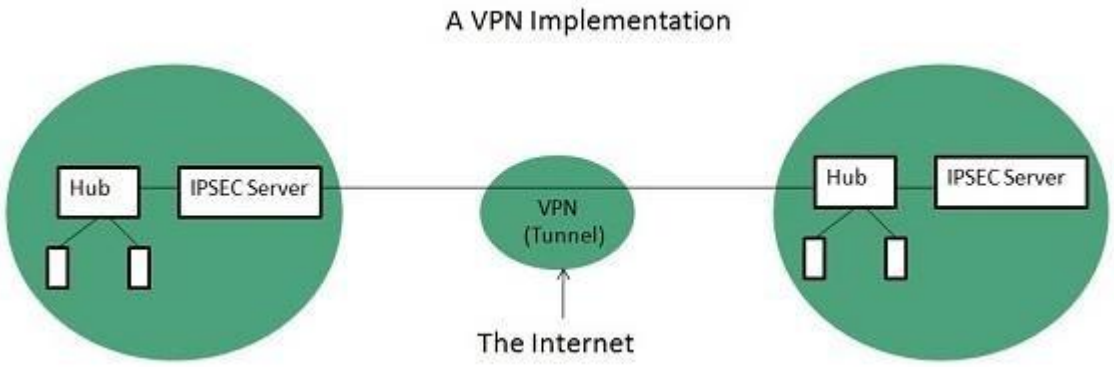


Fig. 5.6. Implementation of extranet

Key Points

- The packet is encapsulated at boundary of networks in IPSEC complaint routers.
- It uses an encryption key to encapsulate packets and IP addresses as well.
- The packet is decoded only by the IPSEC complaint routers or servers.
- The message is sent over VPN via VPN Tunnel and this process is known as tunneling.

- **Uses of Extranet**
- Exchange large volumes of data using EDI
- Share product catalogs exclusively with wholesalers or those in the trade.
- Collaborate with other companies on joint development efforts.
- Jointly develop and use training programs with other companies.

Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affilitated banks.

- Share news of common interest exclusively with partner companies.

Extranet vs. Intranet

The following table shows differences between Extranet and Intranet:

Extranet	**Intranet**
Internal network that can be accessed externally.	Internal network that can not be accessed externally.
Extranet is extension of company's Intranet.	Only limited users of a company.
For limited external communication between customers, suppliers and business partners.	Only for communication within a company.

5.7 VPN

VPN is *a*networkthat is constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network. There are a number of systems that enable you to create networks using theInternetas the medium for transporting data. These systems useencryptionand othersecuritymechanisms to ensure that onlyauthorizedusers can access the network and that the data cannot be intercepted.

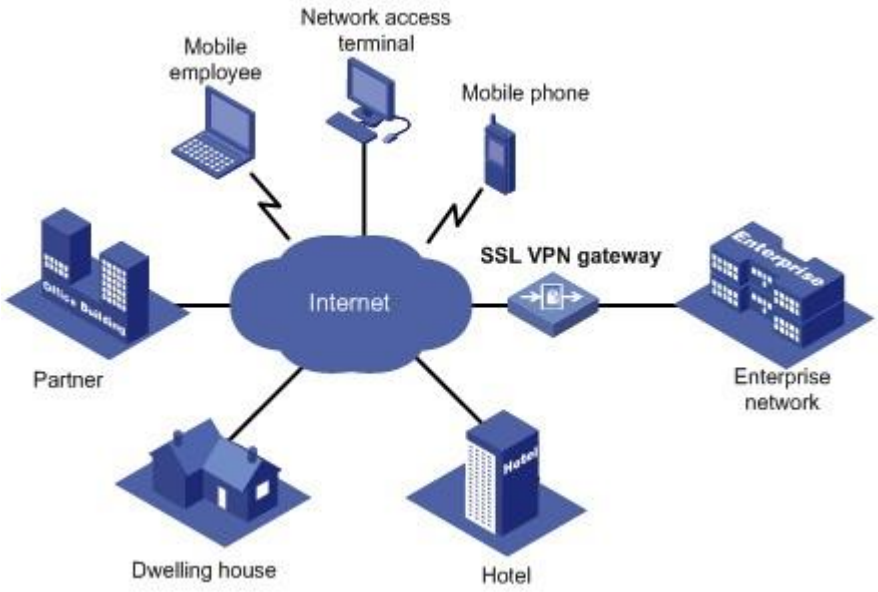


Fig.5.7. VPN

Type of VPN

Early data networks allowed VPN-style remote connectivity throughdial-up modemsor throughleased lineconnections utilizingFrame RelayandAsynchronous Transfer Mode(ATM) virtual circuits, provisioned through a network owned and operated bytelecommunication carriers. These networks are not considered true VPNs because they passively secure the data being transmitted by the creation of logical data streams. They have been replaced by VPNs based on IP and IP/Multiprotocol Label Switching(MPLS) Networks, due to significant cost-reductions and increased bandwidth provided by new technologies such as Digital Subscriber Line (DSL) and fiber-optic networks.

VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). In a corporate setting, remote-access VPNs allow employees to access their company'sintranetfrom home or while traveling outside the office, and site-tosite VPNs allow employees in geographically disparate offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, twoIPv6networks over anIPv4network.

VPN systems may be classified by:

- Theprotocolsused totunnelthe traffic.
- The tunnel's termination point location, e.g., on the customeredgeor network-provider edge.

- Whether they offer site-to-site or network-to-network connectivity.
- The levels of security provided.
- TheOSI layerthey present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity.

Security Mechanisms

To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use ofencryptiontechniques.

VPNs provide security by the use oftunneling protocolsand through security procedures such asencryption. The VPN security model provides:

- confidentialitysuch that even if the network traffic is sniffed at the packet level an attacker would only seeencrypted data
- Senderauthenticationto prevent unauthorized users from accessing the VPN.
- Messageintegrityto detect any instances of tampering with transmitted messages.

Secure VPN protocols include the following:

- **Internet Protocol Security(IPsec)** as initially developed by the Internet Engineering Task Force (IETF) forIPv6, which was required in all standards-compliant implementations ofIPv6beforeRFC 6434made it only a recommendation. This standards-based security protocol is also widely used withIPv4and theLayer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- **Transport Layer Security(SSL/TLS)** cantunnelan entire network's traffic or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble withNetwork Address Translationand firewall rules.
- **Datagram Transport Layer Security(DTLS)** - used inCisco Any Connect VPNand inOpen Connect VPNto solve the issuesSSL/TLShas with tunneling overUDP.
- **Microsoft Point-to-Point Encryption(MPPE)** works with thePoint-to-Point TunnelingProtocoland in several compatible implementations on other platforms.
- **MicrosoftSecure Socket Tunneling Protocol(SSTP)** tunnelsPoint-to-Point Protocol (PPP)orLayer 2 Tunneling Protocoltraffic through anSSL3.0 channel. (SSTP was introduced inWindows Server 2008and inWindows VistaService Pack 1.)
- **Multi Path Virtual Private Network (MPVPN).**Ragula Systems Development Company owns the registeredtrademark"MPVPN".
- **Secure Shell (SSH)VPN** -OpenSSHoffers VPN tunneling (distinct fromport forwarding) to secure remote connections to a network or to inter-network links. OpenSSH server

provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

Authentication

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may usepasswords,biometrics,two-factor authentication or othercryptographicmethods. Network-to-network tunnels often use passwords ordigital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the user.

Tunneling

Tunneling is the transmission of data through a public network in such way that routing nodes in the public network are unaware that the transmission is part of a private network.

Tunneling is generally done by encapsulating the private network data and protocol information within the public network protocol data so that the tunneled data is not available to anyone examining the transmitted data frames.

Tunneling allows the use of public network to carry data on behalf of users as though they accessed to a private network.

Advantages of VPN

VPN can provide benefits for an organization. It can

- Extend geographic connectivity.
- Improve security where data lines have not been ciphered.
- Reduce operational costs vs. traditional costs.
- Reduce transit time and transportation costs for remote users.
- Simplify network topology in certain scenarios.
- Private global networking opportunities.
- Provide telecommunication support.
- Provide broadband networking compatibility.
- Provide faster ROI (return on investment) than traditional carrier leased/ owned WAN lines.
- Show good economy of scale.
- Scale well, when used with a public key infrastructure.

5.8 Firewall

A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. a firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied.

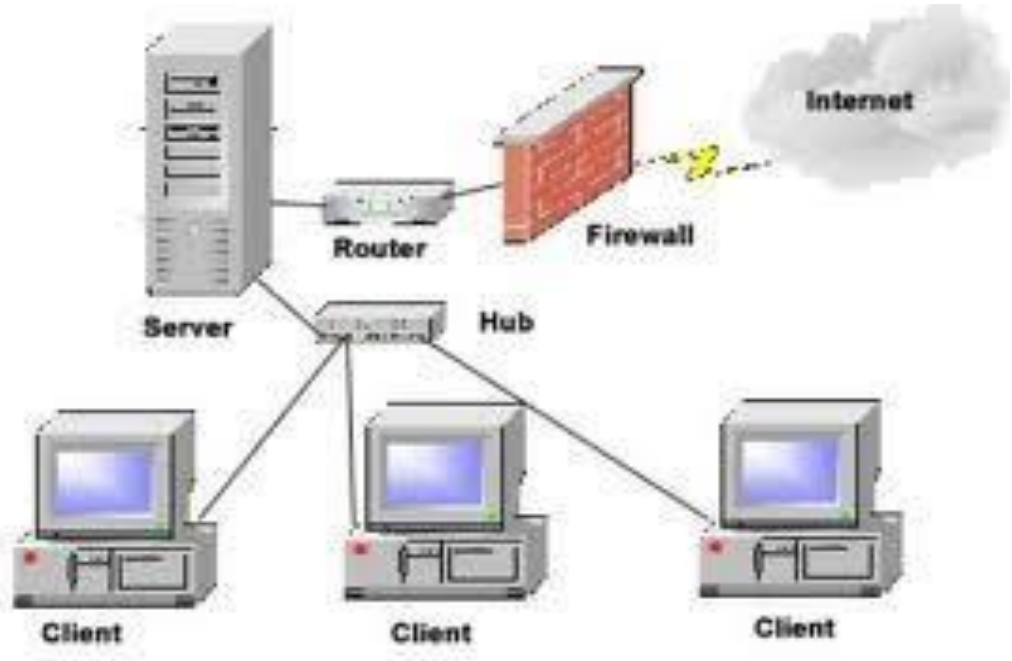


Fig. 5.8. Firewall

Types of firewalls:-

- **Packet filter firewalls:-**

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port numberare checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped (i.e., not forwarded to their destination). Packet-filter firewalls work mainly on the first three layers of the OSIreference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port number

For example, if a firewall is configured with a rule to block Telnetaccess, then the firewall will drop packets destined for TCPport number 23, the port where a Telnet server application would be listening.

Advantage:-

- The primary advantage of packet-filtering firewalls is that they are located in just about every device on the network. Routers, switches, wireless access points, Virtual Private Network (VPN) concentrators, and so on may all have the capability of being a packet-filtering firewall.
- The Biggest Advantage of Packet Filtering Firewalls is Cost and Lower Resource Usage and best suited for Smaller Networks

Disadvantage:

- Packet-filtering firewalls *do not* have visibility into the payload.
- Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule based models. And it‘s also Vulnerable to Spoofing in some Cases.

➢ **Stateful Inspection**

Stateful inspection takes the basic principles of packet filtering and adds the concept of history, so that the firewall considers the packets in the context of previous packets. For example it records when it sees a TCP SYN packet in an internal table and in many implementations will only allow TCP packets that match an existing conversation to be forwarded to the network.

Advantages

- It is possible to build up firewall rules for protocols which cannot be properly controlled by packet filtering.
- Complete control traffic is possible.

Disadvantages

- In stateful inspection implementation is necessarily more complex and therefore more likely to be buggy.
- It also requires a device with more memory and a more powerful CPU etc for a given traffic flow seen over a period of time.

Network Address Translation

Network Address Translation *(NAT)* is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

NAT can be used to allow selective access to the outside of the network, too. Workstations or other computers requiring special access outside the network can be assigned specific external IPs using NAT, allowing them to communicate with computers and applications that require a unique public IP address. Again, the firewall acts as the intermediary, and can control the session in both directions, restricting port access and protocols.

NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

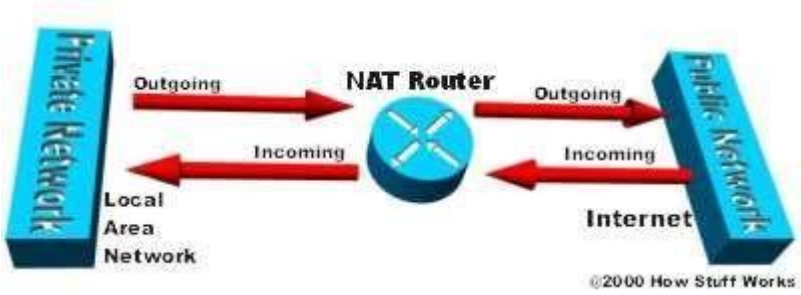


Fig. 5.9. NAT

5.9 Cryptography

Cryptography is the process through which to achieving security by encoding messages to make them non-readable.

Plain Text: Clear text or plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Cipher Text: When a plain text message is modified using any suitable scheme to protect its secrecy, the resulting message is called as cipher text.

Encryption converts plain text to cipher text,**decryption** converts cipher text to plain text.

Cryptography is used to achieve information:

- **Confidentiality** – only authorized persons can achieve information.
- **Integrity** – information that was sent is what was received.
- **Authentication** – guarantee of originator and of electronic transmission.
- **Non repudiation**- originator of information cannot deny any content or transmission.

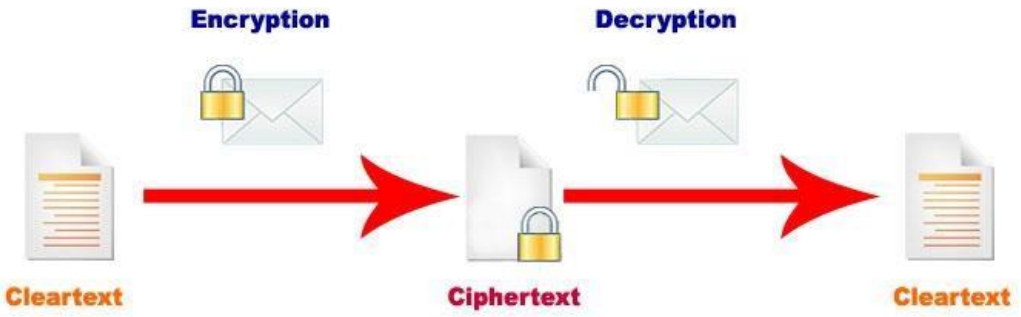


Fig. 5.10.Cryptography

Methods of Cryptography:

❖**Private key Cryptography**

In Private key Cryptography, the sender and recipient agree beforehand on a secret private key. The plain text is somehow combined with the key to create the cipher text. The method of combination is such that, it is hoped, an advisory could not determine the meaning of the message without decrypting the message, for which he needs the key. Private key methods are efficient and difficult to break. The key must be exchanged between the sender and recipient.

❖**Public key Cryptography**

In Public key Cryptography there is also a private key and in private key cryptography this key is used to decrypt the cipher text. In public key cryptography only the recipient has the private key. The sender has a public key anyone who wants to send an encrypted message to the recipient can use the public key. Public key Cryptography depends upon the one way functions. One way function s is a function that is easy to apply but extremely difficult to invert. The public key algorithm uses a one way function to translate plain text to cipher text. Then without the private key it is very difficult for anyone to reverse the process.

5.10 Digital Signature

A digital signature is a stream of bits appended to a document . the purpose of a digital signature is to provide assurance about the origin of the message and the integrity of the message contents. When a message with a digital signature is transmitted and received , the following parties are involved:

- The signer who signs the document.
- The verifier who receives the signed document and verifies the signature.
- The arbitrator who arbitrates any disputes between the signer and the verifier if there is a disagreement on the validity of the digital signature.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signature are easily transportable can be limited by someone else and can be automatically time-stamped.

How it works

Assume you send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was changed from what you sent and that is a really from you.

- Copy and paste the contract into an email note.
- Using special software, you obtain a message hash (mathematical summery) of the

contract.

- Then use a private key that you have previously obtained from a publicprivate key authority to encrypt the hash.
- The encrypted hash becomes your digital signature of the message.
- Some other issuing information related to encryption includes:

- Secure socket layer (SSL) protocols which allow for the transmission of encrypted data access the internet by running above the TCP/IP protocols.
- The effectiveness and easily accessible security technology such as PGP.
- Other uses of encryption such as access controls and watermarks.
- The technical means by which keys use hash table s to achieve the encryption and decryption process.
- Regulation of certificate authorities (CAs), registration authorities that validate users as having been issued certificates and he directories that store certificates, public keys and certificate management information.
- Policies that identify how an institution manages certificates for its own personnel, including legal liabilities and limitations, standards on contents of certificates and actual user practices.

5.11 Digital Envelope

Digital enveloping is an application in which the sender sends the message in such a way that no one other than the intended recipient can open sealed message. It uses both symmetric and asymmetric encryption algorithm.

Sender encrypts the message with receiver‘s public key using some asymmetric algorithm and sends the message to receiver. Since he message is encrypted with a public key, it can be decrypted with complaint key in the same key-pair which is receiver‘s private key and only receiver knows it. Even though the hacker can eavesdrop the cipher text he won‘t know what the actual message that is being sent is.

Asymmetric encryption is 1000 times slower than the symmetric application.

5.12 Digital Certificates

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority.

The implementation of digital certification involves signature algorithm that both hashes the message and signs the hash with the private key rather than using a message digest function followed by message digest encryption algorithm.

There are two types of digital certificates, such as

- **Server certificates** are used to authenticate the identity of websites to make sure that there is no impersonation. They facilitate the exchange of personal information like credit card numbers among website visitors. Server certificate are a necessary for ecommerce site that facilitates the exchange of confidential information among customers, vendors and clients.
- Personal certificates are used to authenticate visitors, identity and restrict their access to specific content. These certificates are suitable for B2B transaction like inventory management, updating product availability, shipping dates and so on.

The working of digital certificates is based on private/ public key technology. Each of these keys is a unique encryption device. Since two keys are never similar, these keys can be used to find the identity of the user. These keys are always work in pairs. The private key is kept secret while the public key is distributed among the different users who want to communicate. Whatever data is encrypted by the public key can only be decrypted by the private key.

Certification Authorities:

Certificates are signed by the Certificate Authority (CA) that issues them. In essence, a CA is a commonly trusted third party that is relied upon to verify the matching of public keys to identity, e-mail name, or other such information.

A certificate shows that a public key stored in the certificate belongs to the subject of that certificate. A CA is responsible for verifying the identity of a requesting entity before issuing a certificate. The CA then signs the certificate using its private key, which is used to verify the certificate. A CA's public keys are distributed in software packages such as Web browsers and operating systems, or they can also be added manually by the user.

Types of Digital Certificates:

There are three types of digital certificate such as :

1. Type I digital certificate
2. Type II digital certificate 3.Type III digital certificate

1. **Type I digital certificate:**

These types of digital certificate authenticate only e-mail and are not legally recognized in India as per the IT Act 2002.

2. **Type II digital certificate:**

These types of digital certificate authenticate e-mail, name and identity and are legally recognized in India as per the IT Act 2002.

3. **Type III digital certificate:**

These are used to authenticate e-mail, name and identity and are globally interoperable. These certificates are legally recognized in India as per IT Act 2002.

5.13 Contents

❖**Hypertext**

Hypertext is text which contains links to other texts. The term was coined by Ted Nelson around 1965. Hypermedia is a term used for hypertext which is not constrained to be text: it can include graphics, video and sound, for example. Apparently Ted Nelson was the first to use this term.

❖**HTML**

Html or hyper textmarkup language is the standard markup language used to create web pages. Html is written in the form of html elements consisting of tags enclosed in angle brackets (like <html>).amarkup language is a set of markup tags. Each html tag describes different document content.

❖**HTTP**

HTTP stands for Hypertext transfer Protocol. It is the set of rules or protocol that governs the transfer of hyper text between two or more computers. HTTP also provides access to other internet protocols such as

- FTP(file transfer protocol)
- SMTP(simple mail transfer protocol)
- NNTP(network news transfer protocol)
- WAIS
- Gopher
- Telnet

CHAPTER - 6
ELECTRONIC PAYMENT SYSTEM

6.1 Introduction

E-commerce is growing rapidly and many merchants are asking themselves how they can benefit from this new technology.

Problems with traditional payment system:-

Lack of convenience:-

Traditional payment systems require the customer to either send paper cheques by snail-mail or require him/her to physically come over and sign papers before performing transaction.

- Lack of security:-

This is because the customer has to send all confidential data on a paper, which is not encrypted that too by post where it may be read by anyone.

- Lack of coverage:-

When we talk in terms of current businesses, they span many countries or states.

Lack of eligibility:-

Not all potential buyers may have a bank account.

6.2 Electronic Payment Mechanism

Electronic Payment System meansofmakingpaymentsover anelectronicnetworksuch as theInternet.

Features of EPS

- There is no paper involved, so electronic payments can be effected directly from home or office.
- Fast, efficient, safe, secure and generally less costly than paper-based alternatives, e.g. cheques.
- Electronic payments are fully traceable.
- Most banks offer same day value for payments made to other accounts held in that same bank.
- Many banks offer same day money transfer inter-bank services for large value payments.
- Unlike cheques, electronic payments don‘t _bounce‘ – as payments will not be effected unless the funds are available in the first place.

6.3 Types of Payment System

❖**Electronic Tokens:-**

An electronic token is a digital analog of various forms of payment backed by a bank or financial institution. Different types of token are

- ***Real time tokens(pre-paid tokens):-***

These are exchanged between buyer and seller their users pre-pay for tokens that serve as currency. Transactions are settled with the exchange of these tokens. Examples of these are dig cash, debit cards etc.

- ***Post paidtokens:-***

These are used with fund transfer instructions between the buyer and seller. Example- electronic cheques, credit card data etc.

❖**Electronic Or Digital Cash:-**

Digital cash is a system of purchasing cash credits in relatively small amounts, storing the credits in your computer, and then spending them when making electronic purchases over the Internet.

Some qualities of cash are

- Cash is a legal tender i.e. payee is obligatory to take it.
- It is negotiable i.e. can be given or traded to someone else.
- It is a bearer instrument i.e. possession is proof of ownership.
- It can be held and used by anyone, even those without a bank certificate.
- It places no risk on part of acceptor.

The following are the limitation of debit and credit card:-

- They are identification cards owned by the issuer and restricted to one user i.e cannot be given away.
- They are not legal tender.
- Their usage requires an account relationship and authorization system.

Properties of digital cash must

- have a monetary value must be
- interoperable or exchangeable must
- ne storable and retrievable:
- should not be easy to copy or tamper

❖**Electronic Cheques:-**

The electronic cheques are modelled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer‘s bank and bank account. The are delivered either by direct transmission using telephone lines or by public networks such as the internet.

Benefits of electronic cheques:-

- Well suited for cleaning micro payments. Conventional cryptography of e-cheques makes them easier to process than systems based on public key cryptography(like digital cash).
- They can serve corporate markets. Firms can use them in more cost-effected manner.
- They create float and the availability of float is an important requirement of commerce.

❖**Credit Card** :-

A **credit card** is apayment cardissued to users as a system ofpayment. It allows thecardholderto pay for goods and services based on the holder's promise to pay for them. The issuer of the card creates arevolving accountand grants aline of creditto the consumer(or the user) from which the user can borrow money for payment to amerchantor as acash advanceto the user.

A credit card issuing company, such as a bank or credit union, would enter into agreements with merchants for them to accept their credit cards.

How credit card works:-

- Credit cards work in an e-government application as they work in the physical world. Citizens enter credit card information into a web application to pay for goods or services.
- Government‘s credit card application should invoke required data and business-rules edits to validate online data elements. Some of the edits could include user name, password, merchant ID, account number, expiration date, amount, and customerbilling data.
- Once the validity of required data has passed the credit card application edits the authentication of the cardholder‘s card ID and account number must be validated, and the transaction amount must be within the cardholder‘s credit limits.
- Processor-required elements could include merchant ID account number expiration date amount customer-billing data, card type and card verification value (CVV).
- When all required edits are passed, the transaction is transmitted to the credit card processor and associated networks for authorization.
- The credit card-processing network returns an authorization approval which indicates that the credit card is valid and the amount is within the cardholder‘s credit limit.
- A denial code will be returned when the credit card cannot be authenticated or credit limits have been exceeded.
- The opportunity to use another card or some other payment option might be offered.

❖**Debit Card:-**

- Debit cards are also known as check cards. They operate like cash cheque.
- While a credit card is a way to pay later a debit card is a way to pay now. Debit

cards offer an alternative to carrying a check book or cash. Debit means _'subtract'' .In a debit card transaction, theamountof apurchaseis withdrawn from theavailable balancein the cardholder'saccount. If theavailable fundsare insufficient, the transaction is notcompleted. Alsocalledassetcard (in the US), orpaymentcard (in the UK).It has following components like:-Signage
Transaction screen
Card reader
Receipt printer
Audio port
Cassette options
Envelope options(for cash deposition in some machines)

The main **advantages of debit card** are:

- There is no need to carry cash.
- It is quick and less complicated than using a cheque.
- It can also be used for withdrawals of cash.
- Its holders can have a record of the transactions in his bank statement which will enable him to plan and control the expenditure.
- It can be issued to any individual without assessing credit worthiness.

Advantages of electronic payment system

Decreasing technology cost:-

The technology used in the networks is decreasing day by day, which is evident from the fact that computers are now dirt-cheap and internet is becoming free almost everywhere in the world.

Reduced operational and processing cost:-

Due to reduced technology cost the processing cost of various commerce activities becomes very less. A very simple reason to prove this is the fact that in electronic transaction we save both paper and time.

Increasing online commerce:-

The above two factors have lead many institution to go online and many others are following them.

Problems in implementing EPS:-

- Preventing double spending: copying the money and spending it several times. This is especially hard to do with anonymous money.
- Making sure that neither the customer nor the merchant can make an unauthorized transaction.
- Preserving customer's confidentiality without allowing customer's fraud.

6.4 Risks Associated with Electronic Payment

Operational risk:-

Operational risk arises from the potential for loss due to significant deficiencies in system reliability or integrity. Operational risk can also arises from customer misuse, and from inadequately designed or implemented electronic banking and electronic money systems.

Credit risk:-

Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks engaging in electronic banking activities may extend credit via non-traditional channels, and expand their market beyond traditional geographic boundaries. Banks engaged in electronic bill payment programs may face credit risk if a third party intermediary fails to carry out its obligations with respect to payment. Banks that purchase electronic money from an issuer in order to resell it to customers are also exposed to credit risk in the event the issuer defaults on its obligation to redeem the electronic money.

Legal risk:-

Legal risk arises from violations of or non-conformance with laws rules regulations or prescribed practices or when the legal rights and obligation of parties to a transaction are not well established. Legal risk may arise from uncertainty about the validity of some agreements formed via electronic media.

6.5 Risk Management option

A risk management process that includes the three basic elements of assessing risks, controlling risk exposure, and monitoring risks will help banks and supervisors attain these goals. Banks may employ such a process when committing to new electronic banking and electronic money activities, and as they evaluate existing commitments to these activities.

Assessing risks:-

Assessing risks is an ongoing process. It typically involves 3 steps:-

- First a bank may engage in a rigorous analytic process to identify risks and where possible, to quantity them. In the event risks cannot be quantified management may still identify how potential risks can arise and the steps it has taken to deal with and limit those risks.
- A second step in assessing risk is for the board of directors or senior management to determine the bank‘s risk, tolerance, based on an assessment of the losses the bank can afford to sustain in the event a given problem materialization.
- Finally management can compare its risk tolerance with its assessment of the magnitude of a risk to ascertain if the risk exposure fits within the tolerance limits.

Managing and controlling risks:-

This phase of a risk management process includes activities such as implementing security policies and measures co-coordinating internal communication, evaluating and upgrading products and services, implementing measures to ensure that outsourcing risks are

controlled and managed, providing disclosures and customer education, and developing contingency plans. Senior management should ensure that staffs responsible for enforcing banking or electronic money activity. Banks increase their ability to control and manage the various risks inherent in any activities when policies and procedures are set out in written documentation and made available to all relevant staff.

Security policies and measures*:-security* is the combination of systems, applications and internal controls used to safeguard the integrity authenticity, and confidentiality of data and operating processes. Proper security relies on the development and implementation of adequate security policies and security measures for processes within the bank, and for communication between the bank and external parties.

A ***security policy***states management‘s intentions to support information security and provides an explanation of the bank‘s security organization. It also establishes guidelines that define the bank‘s security risk tolerance.

Security measuresare combination of hardware and software tools and personnel management which contribute to building secure systems and operations, senior management should regard security as a comprehensive process that is only as strong as the weakest link in the process. Such measures include, for example encryption, passwords, firewalls, virus controls and employee screening. Encryption is the use of cryptographic algorithm to encode clear text data into cipher text to prevent unauthorized observation and passwords pass phrases, personal identification numbers, hardware-based tokens, and biometrics are techniques for controlling access and identifying users.

Monitoring risks:-

For electronic banking and electronic money activities monitoring is particularly important both because the nature of the activities are likely to change rapidly as innovations occur, and because of the reliance of some products on the use of open networks such as the internet.

Two important elements of monitoring are **system testing and auditing:-**

System testing and surveillance:-

Testing of systems operations can help detect unusual activity patter ns and avert major system problems, disruptions, and attacks. Penetration testing focuses upon the identification, isolation, and confirmation of flaws. Surveillance is a form of monitoring in which software and audit applications are used to track activity.

Auditing:-

Auditing internal and external provides an important independent control mechanism for detecting deficiencies and minimizing risks in the provision of electronic banking and electronic money services. The role of an auditor is to ensure that appropriate standards, policies and procedures are developed, and that the bank consistently adheres to them.

Identification, confidentiality & payment integrity

- Each party involved in the transaction must be sure that its counterparty is exactly what she tells she is. People involved must be identified.
- Data exchanged between buyers and sellers must remain confidential.
- Buyers must be certain that the information they get about the payment are reliable.

6.6 Payment Gateway

Payment gateway is a separate service and act as an intermediary between the merchant shopping carts shall the financial n/w involved with transaction including the customer credit card issuer & merchant account.

It checks for validity encrypts transaction details ensure they are sent to the correct destination and then decrypts the responses which are send back to the shopping cart.

A payment gateway can be thought of as digital equivalent to a credit card processing terminal.

This s a seamless process customer doesn‘t directly interact with the gateway as data is forwarded to the gateway via shopping cart and secure SSL connection. The cart is configured via login to sent information in a format that acceptable to the particular gateway.

How payment gateway work :-

Payment gateway encrypt information handle through SSL (Secure socket layer).This prevents opportunity for fraud, and security to transaction process .Gateways communicate with a variety of entities, including:

- The customer
- The merchant (through their website)
- Credit card companies (by verifying information)
- Internet Merchant accounts that relay order information from the gateway to the merchant‘s bank account

Benefits of payment gateway

- **Security:-**
  Gateways keep customer credit card data behind firewalls so that the merchant doesn‘t have to worry about someone ―hacking in‖ to their system.
- **Encryption:-**
  Gateways use SSL encryption to prevent message tampering while the credit card information is being transmitted over the Internet. EMS provides the most secure encryption technology.

- **Back-up redundancy:-**
  Gateways have a backup in place to ensure that merchants can continue processing in the event of an emergency.
- **Up-to-date technology:-**
  Gateways are services that are constantly upgraded to be to date with the latest technology.

6.7 Issues of Electronic Payment Technology

Online payment processing requires coordinating the e flow of transaction among a complex network of financial institution and processors. Online payment processing issues are

- Online payment processing basis
- The payment processing network
- How payment processing works
- What you should know about fraud
- What to look for in a payment processing solution

Online payment processing basis

Online payment processing requires coordinating the flow of transactions among a complex network of financial institutions and processors. Fortunately, technology has simplified this process so that, with the right solution, payment processing is easy, secure, and seamless for both you and your customers.

Purchasing online may seem to be quick and easy, but most consumers give little thought to the process that appears to work instantaneously. For it to work correctly, merchants must connect to a network of banks (both acquiring and issuing banks), processors, and other financial institutions so that paymentinformationprovided by the customer can be routed securely and reliably.

The solution is a payment gateway that connects your online store to these institutions and processors. Because payment information is highly sensitive, trust and confidence are essential elements of any payment transaction. This means the gateway should be provided by a company with in-depth experience in payment processing and security.

The Payment Processing Network

Here‘s a breakdown of the participants and elements involved in processing payments:

Acquiring bank: In the online payment processing world, an acquiring bank provides Internet merchant accounts. A merchant must open an Internet merchant account with an acquiring bank to enable online credit card authorization and payment processing. Examples of acquiring banks include Merchant eSolutions and most major banks.

Authorization: The process by which a customer‘s credit card is verified as active and that they have the credit available to make a transaction. In the online payment processing world, an authorization also verifies that the billing information the customer has provided matches up with the information on record with their credit card company.

Credit card association: A financial institution that provides credit card services that are branded and distributed by customer issuing banks. Examples include Visa® and MasterCard®

Customer: The holder of the payment instrument—such as a credit card, debit card, or electronic check.

Customer issuing bank: A financial institution that provides a customer with a credit card or other payment instrument. Examples include Citibank and Suntrust. During a purchase, the customer issuing bank verifies that the payment information submitted to the merchant is valid and that the customer has the funds or credit limit to make the proposed purchase.

Internet merchant account: A special account with an acquiring bank that allows the merchant to accept credit cards over the Internet. The merchant typically pays a processing fee for each transaction processed, also known as the discount rate. A merchant applies for an Internet merchant account in a process similar to applying for a commercial loan. The fees charged by the acquiring bank will vary.

Merchant: Someone who owns a company that sells products or services.

Payment gateway: A service that provides connectivity among merchants, customers, and financial networks to process authorizations and payments. The service is usually operated by a third-party provider such as VeriSign.

Processor: A large data center that processes credit card transactions and settles funds to merchants. The processor is connected to a merchant‘s site on behalf of an acquiring bank via a payment gateway.

Settlement: The process by which transactions with authorization codes are sent to the processor for payment to the merchant. Settlement is a sort of electronic bookkeeping procedure that causes all funds from captured transactions to be routed to the merchant‘s acquiring bank for deposit.

How payment processing works

Payment processing in the online world is similar to payment processing in the offline or ―Brick and Mortar‖ world, In the online world, the card is ―not present‖ at the transaction. This means that the merchant must take additional steps to verify that the cardinformationis being submitted by the actual owner of the card, Payment processing can be divided into two major phases or steps: authorization and settlement.

Payment Processing—Authorization and Settlement

Authorization verifies that the card is active and that the customer has sufficient credit available to make the transaction. Settlement involves transferring money from the customer‘s account to the merchant‘s account.

Authorization: Online

- ✓ A customer decides to make a purchase on a merchant‘s Web site, proceeds to checkout, and inputs credit card information.
- ✓ The merchant‘s Web site receives customer information and sends transactioninformation to the payment gateway.
- ✓ The payment gateway routes information to the processor.
- ✓ The processor sends information to the issuing bank of the customer‘s credit card.
- ✓ The issuing bank sends the transaction result (authorization or decline) to the processor.
- ✓ The processor routes the transaction result to the payment gateway.
- ✓ The payment gateway passes result information to the merchant.
- ✓ The merchant accepts or rejects the transaction and ships goods if necessary.

Because this is a ―card not present‖ transaction, the merchant should take additional precautions to ensure that the card has not been stolen and that the customer is the actual owner of the card.**Payment Processing—Settlement**

- ✓ The settlement process transfers authorized funds for a transaction from the customer‘s bank account to the merchant‘s bank account.
- ✓ The process is basically the same whether the transaction is conducted online or offline.

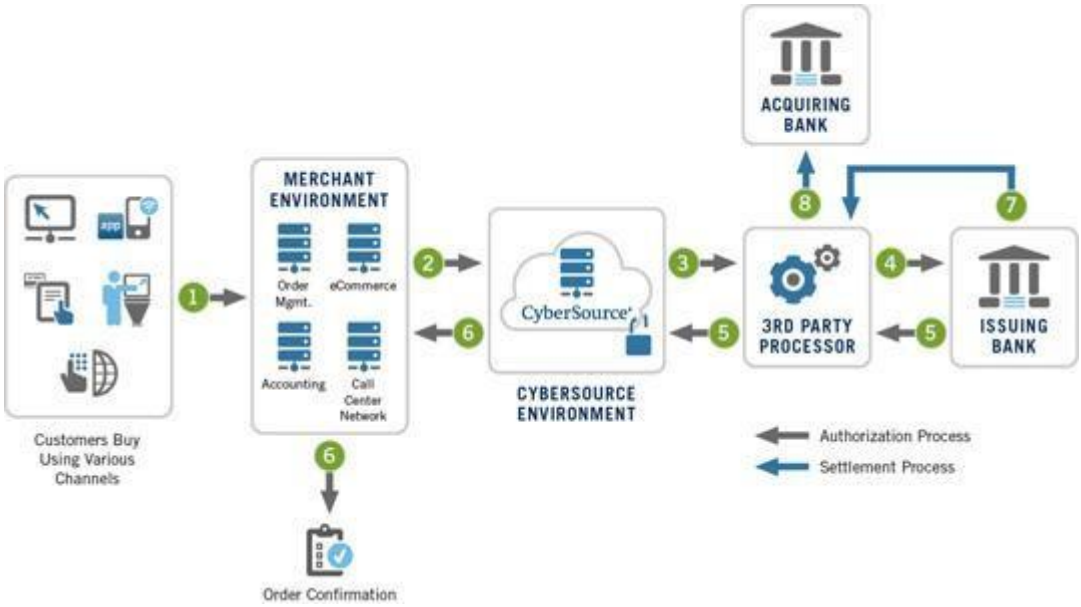


Fig. 6.1.Customer verification

What you should know about fraud

Credit card fraud can be a significant problem for customers , merchants and credit card issuer

6.8 Recommendations

- These recommendation cover payments by clients buying low priced documents, information etc, an clients paying accounts such as rates, license fees etc.
- To minimize liability an agency should outsource both merchant and payment services. Providing there is an adequate contract and a reliable method of updating the agency‘s information on the merchant server, essentially all liability will pass to the merchant service and payment providers who will manage the risks and who can insure against any losses.
- It is important to note that the process of arriving at an adequate contract to achieve this end is no trivial task.
- When an agency succeeds in passing liability to an external provider, it may still suffer serious embarrassment as the only political target for those suffering from a failure in a payment scheme.
- An agency which decides to retain the merchant server in-house but outsource payment services should:
  - Avoid receiving clients details unless encrypted b arrangements between the client and the payment provider.
  - Ensure that advice details passed by the payment provider cannot be repudiated.
  - Install strong access control including firewalling and incident detection measures to prevent hacking of its system. ➢It is assumed that
  - The payment provider will take the necessary steps to avoid system penetration and insure against the risk of failure

- The agency will strenuously protect client if it holds them unencrypted, including perhaps using AISEP-certified software/hardware, particularly for communications between client and agency.

- An agency which decides to operate both merchant and payment servers will need:
  - A highly reliable, preferably AISEP-certified, payments package and agency to financial-instruction communications systems.
  - Strong access control entailing the maximum possible separation between the merchant and the payment servers.
  - Strong protection of both merchant an payment servers against internal and external attacks.
- It is recommended that clients instruct their banks to make the transfer of large payments directly to the agency‘s bank and not use internet-based payments systems.

6.9 Internet Banking

Internet banking refers to systems that enable bank customers to access accounts and general information on bank products and services through PC or other intelligent device.

Internet banking products and services can include wholesale product for corporate customers as well as retail and fiduciary products for consumers. Some example of wholesale products and services include:

- Cash management
- Wire transfer
- Automated clearinghouse transactions
- Bill presentment and payment

Some example of retail and fiduciary products and services include:

- Balance inquiry
- Funds transfer
- Downloading transaction information
- Bill presentment and payment
- Loan application
- Investment activity
- Other value added services

Interbank transfer is a special service that allows you to transfer funds electronically to accounts in other banks through NEFT and RTGS.

NEFT (National Electronic Fund Transfer):- funds are transfer to the credit account with other participating bank using RBI‘s NEFT service. RBI act as a service provider and trans he credit to the other banks account.

RTGS (real time gross settlement):-the RTGS system facilitates transfer of funds from accounts in one bank to another one real time and on gross settlement basis. The RTGS

system fastest possible interbank money transfer facility available through secure banking channel in India.

Minimum /maximum amount for RTGS/NEFT transaction under retail internet banking are:

.

Type	Minimum	Maximum
RTGS	Rs.1 lakh	Rs 5 lakh
NEFT	No limit	Rs 5 lakh

Minimum /maximum amount for RTGS/NEFT transaction under corporate internet banking are:

.

Type	Minimum	Maximum
RTGS	Rs.1 lakh	No limit
NEFT	No limit	No limit

Growth in Internet Banking:-

Various factors including competitive cost, customer service, and demographic considerations are motivating banks to evaluate their technology and assess their electronic commerce and internet banking strategies.

Some of the market factors that may drive a bank‘s strategy include the following:

- **Competition:-** studies show that competitive pressure is the chief driving force behind increasing use of internet banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see internet banking as a way to keep existing customers and attract new ones to the bank. • **Cost efficiencies:-**national banks can deliver banking services on the internet at transaction costs far lower than traditional brick-and –mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used.
- **Geographical reach:-** internet banking allows expanded customer contact through increased geographical reach and lower cost delivery channels. In fact some banks are doing business exclusively via the internet—they do not have traditional banking offices and only reach their customers online.
- **Branding:-** relationship building is a strategic priority for many national banks. Internet banking technology and products can provide a means for national banks to develop and maintain an ongoing relationship with their customers by offering easy access to broad array of products and services. By capitalizing on brand identification and by providing a broad array of financial services, banks hope to build customer loyalty, cross-sell, and enhance repeat business.

- **Customer demographics: -** internet banking allows national banks to offer a wide array of options to their banking customers. Some customers will rely on traditional branches to conduct their banking business. The demographics of banking customers will continue to change. the challenges to national banks is to understand their customer base and find the right mix of delivery channels to deliver products and services profitably to their various market segments.

Types of Internet Banking

Financial institution Internet offerings can be broadly classified into three groups with distinct risk profile.

- **Informational**—Offers information about the bank's products and services ("brochure ware") and is low risk
- **Communicative**—Offers account-related information and possibly offers updates to static data (such as addresses). Since access is permitted to the bank's main systems, the risk is material.
- **Transactional**—Allows customers to execute financial transactions and carries the highest risk. Some transactional models carry higher risks; for example, if the customer has never visited a branch throughout his entire relationship and prefers to carry out all his transactions remotely (this commonly happens with some online share trading sites).

Internet Banking Risks

Internet banking does not open up new risk categories, but rather accentuates the risks that any financial institution faces. The board and senior management must be cognizant of these risks and deal with them appropriately. These risks, which often overlap, are briefly described below:

- **Strategic risk**— This is the current and prospective risk to earnings and capital arising from adverse business decisions or improper implementation of business decisions. Many senior managers do not fully understand the strategic and technical aspects of Internet banking. Spurred by competitive and peer pressures, banks may seek to introduce or expand Internet banking without an adequate cost-benefit analysis. The organization structure and resources may not have the skills to manage Internet banking.
- **Transaction risk**— This is the current and prospective risk to earnings and capital arising from fraud, error, negligence and the inability to maintain expected service levels. A high level of transaction risk may exist with Internet banking products, because of the need to have sophisticated internal controls and constant availability. Most Internet banking platforms are based on new platforms which use complex interfaces to link with legacy systems, thereby increasing risk of transaction errors.

There is also a need to ensure data integrity and non-repudiation of transactions. Third-party providers also increase transaction risks, since the organization does not have full control over a third party. Without seamless process and system connections between the bank and the third party, there is a higher risk of transaction errors.

- **Compliance risk**— This is the risk to earnings or capital arising from violations of, or nonconformance with, laws, regulations and ethical standards. Compliance risk may lead to diminished reputation, actual monetary losses and reduced business opportunities. Banks need to carefully understand and interpret existing laws as they apply to Internet banking and ensure consistency with other channels such as branch banking. This risk is amplified when the customer, the bank and the transaction are in more than one country. Conflicting laws, tax procedures and reporting requirements across different jurisdictions add to the risk. The need to keep customer data private and seek customers' consent before sharing the data also adds to compliance risk. Customers are very concerned about the privacy of their data and banks need to be seen as reliable guardians of such data. Finally, the need to consummate transactions immediately (straight-through processing) may lead to banks relaxing traditional controls, which aim to reduce compliance risk.
- **Reputation risk**— This is the current and prospective risk to earnings and capital arising from negative public opinion. A bank's reputation can be damaged by Internet banking services that are poorly executed (e.g., limited availability, buggy software, poor response). Customers are less forgiving of any problems and thus there are more stringent performance expectations from the Internet channel. Hypertext links could link a bank's site to other sites and may reflect an implicit endorsement of the other sites.
- **Information security risk**— This is the risk to earnings and capital arising out of lax information security processes, thus exposing the institution to malicious hacker or insider attacks, viruses, denial-of-service attacks, data theft, data destruction and fraud. The speed of change of technology and the fact that the Internet channel is accessible universally makes this risk especially critical.
- **Credit risk**— This is the risk to earnings or capital from a customer's failure to meet his financial obligations. Internet banking enables customers to apply for credit from anywhere in the world. Banks will find it extremely difficult to verify the identity of the customer, if they intend to offer instant credit through the Internet. Verifying collateral and perfecting security agreements are also difficult. Finally, there could be questions of which country's (or state's) jurisdiction applies to the transaction.
- **Interest rate risk**— This is the risk to earnings or capital arising from movements in interest rates (e.g., interest rate differentials between assets and liabilities and how these are impacted by interest rate changes). Internet banking can attract loans and deposits from a larger pool of customers. Also, given that it is easy to compare rates across banks, pressure on interest rates is higher, accentuating the need to react quickly to changing interest rates in the market.
- **Liquidity risk**— This is the risk to earnings or capital arising from a bank's inability to meet its obligations. Internet banking can increase deposit and asset volatility,

especially from customers who maintain accounts solely because they are getting a better rate. These customers tend to pull out of the relationship if they get a slightly better rate elsewhere.

- **Price risk**— This is the risk to earnings or capital arising from changes in the value of traded portfolios or financial instruments. Banks may be exposed to price risk, if they create or expand deposit brokering, loan sales or securitization programs as a result of Internet banking activities.
- **Foreign exchange risk**— This arises when assets in one currency are funded by liabilities in another. Internet banking may encourage residents of other countries to transact in their domestic currencies. Due to the ease and lower cost of transacting, it may also lead customers to take speculative positions in various currencies. Higher holdings and transactions in nondomestic currencies increase foreign exchange risk.

Risk management:-

Financial, institutions have a technology risk management process to enable them to identify, measure, monitor, and control their technology risk exposure. Risk managements of a new technologies has three essential elements

- The planning process for the use of the technology.
- Implementation of the technology.
- The means to measure and monitor risk.

The risk planning process is the responsibility of the board and senior management. They need to process the knowledge and skills to manage the banks use of internet banking technology and technology-related risks. The board should review, approve, monitor internet banking technology-related projects that may have a significant impact on the banks risk profile. They should determine whether the technology and products are in line with in banks strategic goals and met a need in their market. senior management should have the skills to evaluates the technology employed and risks assumed

Periodic independent evaluations of the internet banking technology and products by auditors or consultants can helps the board and senior managements fulfil their responsibilities

Implementing the technology is the responsibility of management. Management should help the skills to effectively evaluate internet banking technologies and products, select the right mix for the bank, and see that they are installed appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting with a vendor how specializes in this type of business or engaging in an alliance with another provider with complementary technologies or expertise.

Measuring and monitoring the risks is the responsibility of management. Management should have the skills to effectively identify measure, monitor and control risks associated with internet banking. The board should receive regular reports on the technologies employed, the risks assumed, and how dose risks are managed. Monitoring system performance is the keys success factor. As part of the designed process, in national bank should include effective quality assurance and audit processes in its internet banking system. The bank should periodically review the systems to determine whether they are meeting the performance standards.

Internal controls:-

Internal controls over internet banking system should be commensurate with an institutions level of risks. Management has the ultimate responsibility for developing and implementing around system of internal controls over the banks internet banking technology and product

Regular audits of the control systems will help ensure that the controls are appropriate and functioning properly. For example the control objective for an individual's banks internet banking technology and product might focus on

- Consistency of technology planning and strategic goals, including efficiency and economic of operation and compliance with corporate policies legal requirements
- Data availability , including business recovery planning
- Data integrity including providing for the safeguarding of asset, proper authorization of transactions, and reliability of process and output.
- Data confidentiality and privacy safe guards.
- Reliability of MIS.

Once control objectives are established, management has the responsibility to install the necessary internal controls to see that the objectives are met. Management also has the responsibility to evaluate the appropriateness of the control on a cost-benefit basis.

According to the information systems audit and control association (ISACA) basic internal the basic internal components include:-

- **Internal accounting controls:-U**sed to safeguard the assets and reliability of financial records. This would include transaction records and trial balances
- **Operational controls:-U**sed to ensure those business objectives are the met. this would include operating plans and budges to compare actual against planned performance
- **Administrative controls:-U**sed to ensure operational efficiency and adherence to policies and procedures .this would include periodic internal and external audits.
- **Preventing control:-P**revent something(often an error or illegal act)from happing .An example of this type of control is logical access control software that would allow only authorized person to access a network using a combination of a user id and password.
- **Detective controls:-I**dentify an action that has occurred. An example would be intrusion detection software that triggers an alert all alarm.
- **Corrective control:-C**orrect a situation once it has been detected. an example would be software back up that could be used to recover a corrupted file or database. Banks or service providers offering transaction –based internet banking product need to have high level of controls to help manage the banks transaction risk.

  Example of this control could include
- Monitoring transaction activity to look for anomalies in transaction types , transaction volumes ,transaction values and time – of-day presentment

- Monitoring log-on violation or attempts to identify patterns of suspect activity including unusual request ,unusual timing or unusual formats.
- Using trap and trace techniques to identify the source of the request and match this against known customers

Regular reporting and review of unusual transactions will help identify

- Intrusions by unauthorized parties
- Customer input errors
- Opportunities for customer education

6.10 Security Requirement of Electronic Payment System

➢Authentication

Authentication is the process of determining the true identity of buyer‘s before payments are made. Authentication is also used in other ways - not just for identifying users, but also for identifying devices and data messages.

Authentication is an important issue in an internet banking systems. Banks use symmetric encryption technology to secure messages and asymmetric encryption to authenticate parties.

Biometric devices are an advanced form of authentication. These devices may take the form of a retina scan, figure or thumb print scan, facial scan, or voice print scan. Biometrics may be used by some banks for authentication.

➢Trust

Another issue in internet banking is trust. Public and private key cryptography systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party certificate authority is necessary part of the process. A certificate authority is a trusted third party that verifies identities in cyberspace.

➢Privacy

The important issue for a consumer is privacy. National banks that recognize and respond to privacy issues in a proactive way make this positive attribute for the bank and a benefit for its customers.

➢Non-repudiation

Non-repudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the public key encryption was developed, i.e. to authenticate electronic message and prevent denial or repudiation by the sender or receiver. Although technology has provided an answer to non-repudiation, and state laws are not uniform in the treatment of electronic authentication and digital signature.

➢Availability

Availability is another component in maintaining a high level of public confidence in an environment. Users of a network expect access to system 24 hours per day, seven days in a week. Among the consideration associated with system availability are capacity, performance monitoring, and redundance and business resumption.

Performance monitoring technique will provide management with information

such as the volume of traffic, the duration of transaction and the amount of time customers must wait for service. Monitoring capacity, downtime and performance on a regular basis will help management assure a high level of availability for their internet banking systems.

6.11 Secure Socket Layer

Secure Socket Layer is a protocol developed by Netscape for transmitting private documents via the internet. SSL uses a cryptographic system that uses two keys to encrypt data, a public key known to every one and a private or secret key known only to the recipient of the message.

To ensure privacy of information both the client and the server must run compatible security schemes.

Authentication is used for identifying the clients as well as the server in a network environment. Client authentication refers to the identification of a client by a server. Server authentication refers to identification of a server by a client.

The technology used to provide secure channel over the web are SSL and S-HTTP (secure hyper text transfer protocol).

The SSL provides end-to-end secure data transmission between the web server and the web client.SSL secures only web sessions and not e-mail or file transfer sessions. The SSL ensures secure data transfer but is not responsible for security of data residing in the web client or server.

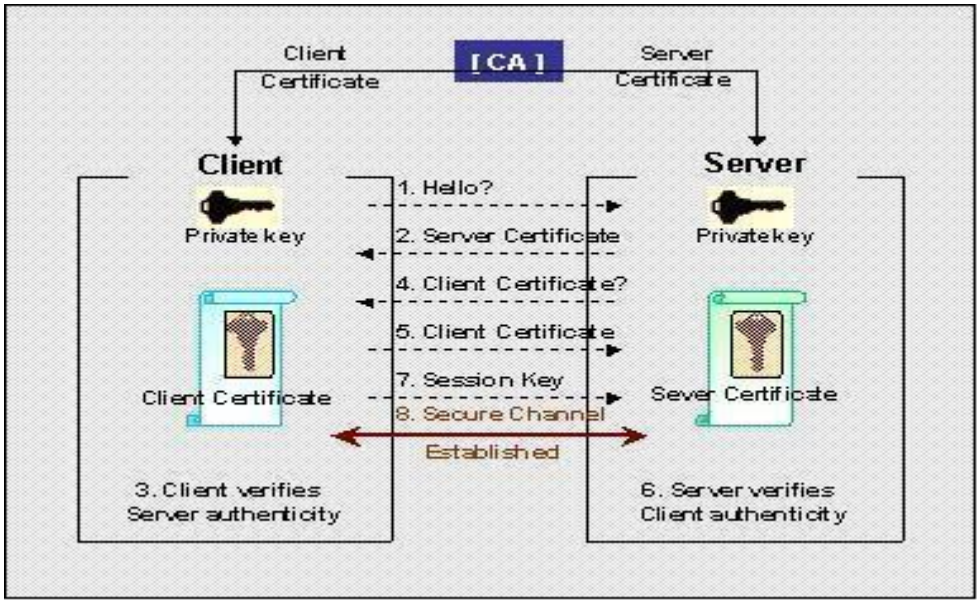


Fig. 6.2. SSL

How SSL works

The SSL performs two functions using either symmetric encryption or asymmetric encryption.

- Authenticate the websites.
- Ensures secure data transmission between the web server and the client.

In symmetric encryption, a key called the private key is used both for encrypting is called the public key and the one used to decrypt is called private key. For symmetric encryption to work, the sender and the receiver should share the secret key. This is possible only when the sender and receivers know each other.

In asymmetric encryption two separate keys are used to encrypt and decrypt data. The public key is shared with the other person and the private key is known only to the person who decrypts‘ the data. So the private key will remain a secret while the public key will be known to both the parties.

Secure Hyper Text Transfer Protocol (SHTTP)

S-HTTP enables secure communication between the web server and the client that allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains adigital certificate, or both. S-HTTP was developed to support several esecurity technologies like symmetric encryption for data confidentiality, message digest for data integrity and PKI encryption. These technologies can be used individually or in combination. It can be set to required, optional, or refused.

If the security property is required, include the type of technology to be used, the algorithms that will be supported, and the direction in which the property is to be enforced.

If the security property has been set to optional, it means that the security property is not mandatory for making connections.

If the security property is set to refuse, then it means that the negotiating party cannot enforce this property.

Once the secure property has been set then the data is encapsulated.

Secure Electronic Transaction (SET)

The secure electronic transaction (SET) protocol is the protocol used to facilitate the secure transmission of consumer credit card information over insecure networks, such as the Internet. SET blocks out the details of credit card information, thus preventing merchants, hackers and electronic thieves from accessing this information. SET was developed by SETco, led by VISA and MasterCard starting in 1996. The first version was finalized in May 1997 and a pilot test was announced in July 1998.

SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Secure Hypertext Transfer Protocol (S-HTTP).

Authentication Techniques, Processes & Methodology

There are different kind of techniques and methodologies which are available for authentication of an electronic banking product or service.

Shared secrets:-

Shared secrets (something a person knows) are information elements that are known or shared by both the customer and the authenticating entity.

- Questions or queries that require specific customer knowledge to answer, e.g the exact amount of the customer‘s monthly mortgage payment.
- Customer-selected images that must be identified or selected from a pool of images.

The customer‘s selection of a shared secret normally occurs during the initial enrolment process or via an offline ancillary process. Passwords of pin values can be chosen, question can be chosen and responds provided, and images may be uploaded of selected.

Tokens:-

Tokens are physical devices (something the person has) and may be part of a multifactor authentication scheme. Three types of tokens are discussed here:- the USB token device, the smart card, and the password- generating token.

USB token device:-

The USB token device is typically the size of a house key. It plugs directly into a computer‘s USB port and therefore does not require the installation of any special hardware on the user‘s computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB token are one-piece injection-molded devices. USB token are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

Smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. To be used, a smart card must be inserted into a compatible reader attached to the customer‘s computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantages as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer‘s home computer.

Password-Generation Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used.

The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token.

The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if
(1) The regular password matches and
(2) The OTP generated by the token matches the password on the authentication server.

A new OTP is typically generated every 60 seconds- in some systems, every 30 seconds. Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

6.12 BIOMETRICS

The word ―biometrics‖ came from Greek and we can divide it into two roots: ―bio‖ means life and ―metrics‖ – to measure. Biometrics is the process of making sure that the person is who he claims to be. Authentication of identity of the user can be done in 3 three ways:

1) Something that person knows (password),
2) Something the person has (key, special card),
3) Something the person is (fingerprints, footprint).

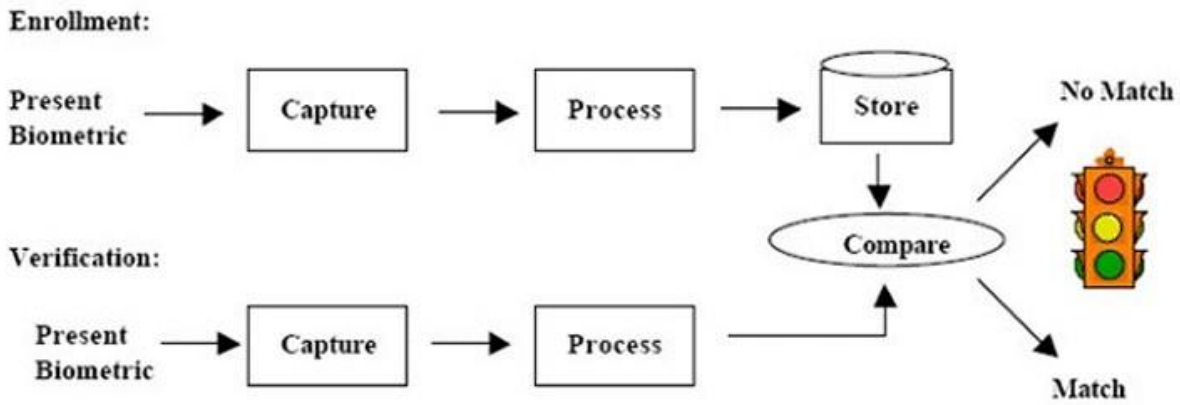


Fig.6.3. Biometrics

Biometrics is based on anatomic uniqueness of a person and as follow it can be used for biometric identification of a person. Unique characteristics can be used to prevent unauthorized access to the system with the help of automated method of biometric control which, by checking unique physiological features or behaviour characteristics identifies the person.

Enrolment

The system captures a characteristic trait from the person, for example his fingerprint, and it processes this information to create an electronic representation called a template. This template is saved in a database, a smart card or in another place that can be accessed during the second step.

Verification

The person tells the system who he is by presenting a card with a magnetic strip, a barcode, or using a PIN or password that only he knows. Immediately, the system asks for a biometric sample. With this sample, the system creates an electronic representation called a live template, which is compared with the reference model saved in the database.

Identification

The person does not tell the system who he is; he uses neither cards nor passwords. The device uses his trait to identify him directly. The system captures this trait and processes it to create a live template. Then, the system compares this with the reference models stored in the database to determine the person‘s identity.

How does Biometrics security works

The largest share of that money (48 percent) goes for fingerprint recognition systems, followed by facial recognition (12 percent). While these two are the most popular, there are other methods that analyze a person's physical or dynamic characteristics. Physical biometric methodologies also look at the following:

Eyes — Examining the lines of the iris or the blood vessels in the retina;

Hands — Taking a 3D image and measuring the height and width of bones and joints, and

Skin — Analyzing surface texture and thickness of skin layers.

When looking at strong authentication, you want two out of three factors — something you have something you are and something you know. While, eyes, hands and skin are commonly used as biometric identifiers, more dynamic methodologies also are being introduced, such as the following: **Voice** — Detects vocal pitch and rhythm;

Keystroke Dynamics — Analyzes the typing speed and rhythm when the user ID and password are entered;

Signature — Matches the signature to one on record, as well as analyzing the speed and pressure used while writing, and

Gait — Measures length of stride and its rhythm.

To keep performance high and storage requirements manageable, today's biometric technologies don't have to store or analyze a complete picture of the body part or the physical feature being used. Imagine the processing power that would be needed to store a highresolutionpicture of someone's face and then compare it with a live imagepixelby pixel. Instead, each method reduces the body part or activity to a few essential parameters and then codes the data, typically as a series of hash marks. For example, a facial recognition system may record only the shape of the nose and the distance between the eyes. That's all the data that needs to be recorded for an individual's passport, **Elements of Biometric system**

- A sensor unit that represents the interface between the user and the machine. This is the point where the biometric trait is acquired.
- A processing unit where the acquired biometric is sampled, segmented and features are being extracted. It also includes quality assurance to determine if the quality of the biometric is good enough to be used further in the process. If the quality of the acquired biometric is poor, the user may be asked to present the biometric again.
- A database unit where the entire enrolled biometric template are being stored and where the templates are being retrieved from in the authentication process.
- A matching unit that compares the newly acquired biometric template with the templates stored in the database and based on decision rule s determine either if the presented biometric is a genuine or if the user is identified or not

Types of Biometric

Biometric characteristics of a person are unique. All biometric identifiers can be divided into two big groups:

1) Physiological
2) Behaviour

Though behaviour biometrics is less expensive and less dangerous for the user, physiological characteristics offer highly exact identification of a person. Nevertheless, all two types provide high level of identification than passwords and cards.

Spheres of use:

- Criminalities (biometric identifiers are used to recognise victims, unidentified body and protection of children against kidnapping.)
- Marketing (methods of biometrics are used to identify owners of loyal cards)
- Time accounting systems at work, schools, etc
- Security systems (areuse to control the access to the rooms and control access to internet resources)
- Voting system (during the functionality of voting system identification/authentication of people, that take part in voting is demanded)
- According to actual international demands (for example, according to the standard of ICAO there should be biometric part in passport.)
- Biometric identifiers are used for registration if immigrants and foreign workers. It allows identifying people even without documents.

- For organisation of distribution of social help.

Methods of biometric authentication differ according their degree of safeness:

- DNA
- Iris recognition18
- Fingerprint
- Face recognition
- Voice
- Typing Rhythm

Physiological Type of Biometrics

Physiological systems are considered to be more reliable as individual features of a person, which are used by these systems, do not change by influence of psycho emotional state. Physiological systems of identification deal with statistical characteristics of a person: fingerprints, iris recognition, hand geometry, DNA, face recognition, palm print.

❖Fingerprints

Fingerprint identification is also known as dactyloskopy or also hand identification is the process of comparing two examples of friction ridge skin impression from human fingers, palm or toes.

Method of fingerprinting helps police to investigate crimes during long period of time. The most amazing fact how many details about person can be known using only his/her fingerprints.

❖Voice Recognition

Voice, like many other characteristics that are used for biometric methods, is unique. Like style of gait, it takes quite little time to analyze the voice and to identify the person.

Voice in biometrics or ―voice print‖ is presented as a numerical model of the sound.

Voice is often compared with fingerprints, because like fingerprints, due to their unique form serve for biometric authentication, so the voice does.

The uniqueness of the voice is achieved due to the different physical components of a human throat and mouth. To produce a sound, air leaves the body of a human being through resonators: larynx, the oral cavity (mouth), nasal cavity (nose).

The form, tone of the sounds is depended on the size of the stream, obstructions. Obstructions may include tongue, gums, teeth, lips, their position and size.

Voice has more than 100 separate characteristics that make voice biometrics to be one of the most reliable. To identify the person with the help of voice print, a sample of speech should be taken. This sample is analyzed. Different multiple measurements are taken and the results are presented in the form of the algorithm.

Common delusion is that the voice itself is 47 stored in the database. No, the output from the algorithm is stored in the database.

For verification, another sample of the speech is taken. As in identification process the second sample is analysed, and measured. If the results match, the identity can be verified.

For voice verification two types of system can be used:

- Text-dependent when the decision is made using speech corresponding text Text-
- independent when there is no use in speech.

Voice print systems differ from each other:

- Fixed password system: all users have one and the same password sentence.
- User-specific text –dependent system: each user has his/her own password
- Vocabulary-dependent system: password is made from fixed vocabulary
- Machine –driven text-independent system: unique text should be pronounced
- User-driven text-independent system: user is free to produce any speech he/she wants.

The first three systems belong to text-dependent type of the system, the last two- to the textindependent.

❖**Gait**

Gait biometrics is a biometrics that is based on the way the person walks. It should be mentioned that gait is not affected by the speed of the person‘s walk.

Some scientists differentiate gait from gait recognition, pointing out that gait can be considered as a cyclic combination of movements that results in human locomotion and gait recognition is recognition of some property style of walk, pathology, etc.

The common parameters of gait analysis are:

- Kinematic parameters such as knee, ankle movements and angles.
- Spatial-temporal parameters as length and width of steps, walking speed.
- Correlation between parameters.
-

There are 3 important properties of human perception of gait:

- Frequency entertainment: various components of the gait share a common
- frequency. Phase locking: the relationships among the components of the gaits
- remain stable. Physical plausibility.

Such characteristic of human being as the ability to identify a person by analyzing the manner of walk is very important for biometrics as it offers more reliable and efficient means for identity verification.

There are three gait recognition approaches:

- ❖ **Machine Vision Based**: this approach includes several digital or analog cameras with suitable optics that are used to acquire the gait data. The image is converted

into black and white image, the feature is extracted from the background, and the system counts light and dark pixels.

- **Floor Sensor:** sensors are situated on a mat along the floor. Walking across the mat the ground measurements starts, also the process is known as GRF (Ground Reaction Force).Gait collection by floor sensors
  - ✓ footsteps recognized,
  - ✓ time spent at each location in footsteps recognized ,✓footsteps profiles for heels and toe strikes, ✓Picture of floor sensor carpet.

- **Wearable Sensor Based:** the new ―word‖ in gait recognition. The approach is based on special motion recoding sensor that a person wears on the body. The sensor can:
  - ✓ Measure acceleration,
  - ✓ Measure rotation and number of degrees per second of rotation, ✓Measure the force of walking.

This approach is used in mobile phones.

❖Iris Recognition

Iris is a unique characteristic of a person. The primary visible characteristic of iris is the trabecular meshwork that makes possible to divide the iris in a radial fashion. It is formed in the eighth month of gestation. Iris is stable and does not change during the whole life.

Iris recognition is considered to be one of the exact methods of biometrics. Iris is protected by eyelid, cornea and aqueous humour that make the likelihood damage minimal unlike fingerprinting.

Some sources divide the process of iris recognition into two steps, some into three:

1. **Capturing the image**: The image can be captured by a standard camera using both visible and infrared light. The procedure can be manual or automated. In the manual procedure the iris should be in focus and the length between the camera and iris should be within six and twelve inches, while in automated procedure the length is between three and a half inches and one metre. In automated procedure the camera automatically locates the face and iris into the focuse and makes the process rather easy and friendly.
2. **Define the location of the iris and optimising the image**: when the iris is in focused, the iris recognition system just identifies the image with the best focus and clarity. The image is analyzed. The purpose of the analysis is to identify the outer boundary of the iris where it meets with white clera of the eye, the pupillary boundary and the centre of pupil. The result of the analysis is the precise location of the circular iris. Iris recognition system tries to identify the areas suitable for feature extraction and analysis: removing areas covered by the eyelids, deep shadows, and reflective areas. This attempt is known as optimisation of the image.
3. **Store and compare the image**: the process of division, filtering and mapping segments of the iris into hundreds of vectors (phasors) takes place. The process is also known as 2-D Gabor. 2-D Gabor phasor can be easily understand as ―what‖ and ―where‖ of the image. Even after this procedure there are still 173 degrees of freedom to identify the iris. 2-D

Gabor takes into consideration the changes that may occur with an iris. Iris image is saved as so-called Iris Code®, 512-byte record. The record is stored in a database.

❖**Hand Geometry**

Hand geometry is the use of geometric shape of the hand for recognition purposes. This method was rather popular 10 years ago but nowadays it is seldom used. The method is based on the fact that the shape of the hand of one person differs from the shape of the hand of another person and does not change after certain age. But it is not unique. The main characteristics for this method are measuring and recording the height, length of the fingers, distance between joints, shape of the knuckles, surface area of the hand.

❖**Facial Recognition**

People used face to distinguish one person from the other. Facial (face) recognition is a computer application that automatically identifies or verifies a person with the help of a digital image or a video frame from a video source. One of the ways to do this is to compare the given example with the examples in the database.

The face of a person has a numerous distinguishable characteristics. Face IT has 80 nodal points and some of these points can be measured by software:

- Distance between eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

By measuring these nodal points a special numeric code is created. This code is called a face print, and it is this code that represents the face in the database.

Facial recognition technologies can be divided into two

- ways: 2-d
- 3-D.

The face recognition process normally consists of four phases:

1. Detecting a face
2. Normalization
3. Feature extraction and recognition
4. Recognise face image

<u>Biometrics Characteristics</u>

- Universality- each person that is using the biometric system should posses the biometric trait
- Uniqueness- measures how well the biometric trait separates one individual form another.
- Performance- measures how well a biometric trait resists aging.

- Collectability- eases of acquisition of the biometric trait without causing inconvenience to the user.
- Performance- accuracy, speed, robustness of technology used
- Acceptability-degree of approval of the biometric technology by the users
- Circumvention- eases of use of an imitation of the biometric treat.

- **Benefits of Biometric System**
- It does not require cooperation.
- It guarantees physical location of the user.
- It has high throughput.
- The biometric trait is unforgettable
- The biometric trait cannot be lost.
- It is cost efficient.
- It can provide emergency identification. It prevents identity theft
- It is appealing.

CHAPTER - 7
SECURITY ISSUES IN E-COMMERCE

7.1 Introduction

Electronic commerce may include any computer mediated business process, but a common usage is to describe commerce taking place using the WWW as an enabling transport.

7.2 E-Commerce Security Issues

- **Access control :** If access control is properly implemented, many other security problems, like lack of privacy ,will either be elimination or mitigated .Access control ensures only those that legitimately require access to resources are given access as well as logical access to resources .Various type of threats exist for access control .
  Example: being able physical to enter a building or having access to network equipment is one example of a threat.
- **Privacy** : privacy ensures that only authorized parties can access information in any system .The information should also not be distributed to parties that should not receive it .Issues related to privacy can be considered as a subset of issues related to access control.
- **Authentication:** Authentication ensures that the origin of an electronic massage is correctly identified. This means having the capability to determine who seen the massage and form where or which machine. Without proper authentication, it will be impossible to know who actually placed on order and whether the order placed is genuine or not.
- **Non-repudiation**: Non repudiation is closely related to authentication and this ensures the sender cannot deny sending a particular massage and the receiver cannot deny receiving a massage. If this happens in frequently, it may not significantly harm e-commerce; however, on a large scale this can be devastating.
- **Availability:** Availability insures that the required systems are available when needed. For an e-commerce sits this means that the customer order systems are available all the time .Two major threats to availability problems are virus attacks and denial of service.

7.3 Risks Involved In E-Commerce

- Carrying out denial-of-service(DOS) attacks that stop access to authorized users of a website, so that the site is forced to offer a reduced level of service or, in some cases, cease operation completely
- Gaining access to sensitive data such as price lists, catalogues and valuable intellectual property, and altering, destroying or copying it
- Altering your website, thereby damaging your image or directing your customers to another site

- Gaining access to financial information about your business or your customers, with a view to perpetrating fraud• Using viruses to corrupt your business data.

Impact upon the business

All of these risks can have a significant impact upon a business running an ecommerce service. The potential business implications of a security incident the following:

- Direct financial loss as a consequences of fraud or litigation.
- Consequential loss as a result of unwelcome publicity.
- Criminal charges if you are found to be in breach of the data protection or computer misuse acts. Or other regulation on e-commerce.
- Loss of market share if customer confidence is affected by a denial-of –service attack, or other.

Risks from viruses, Trojans and worms

- Viruses, Trojan horses and worms are all computer programs that can infect computers.
- Viruses and worms spread across computers and networks by making copies of them, usually without the knowledge of the computer user.
- A Trojan horse is a program that appears to be legitimate but actually contains another program or block of undesired malicious, destructive code, disguised and hidden in a block of desirable code.
- A black-door Trojan is a program that allows a remote user or hacker to bypass the normal access controls of a computer and gives them unauthorized control over it. Typically a virus is used to place the back-door Trojan onto a computer, and once the computer is online, the person who sent the Trojan can run programs on the infected computer, access personal files, and modify and upload files.

Risks to e-commerce systems:-

- Corrupting or deleting data on the hard disk of your server.
- Stealing confidential data by enabling hackers to record user keystrokes.
- Enabling hackers to hijack your system and use it for their purpose.
- Using your computer for malicious purpose, such as carrying out a denial-of –service (DOS) attack on another website.
- Harming customer and trading partner relationships by forwarding viruses to them from your own system.

Spyware

Spyware is software that is placed on your computer when you visit certain websites. It is used to secretly gather information about your usage and sends it back to advertisers or other interested parties. In addition to tracking your system use, it can also slow down or crash your computer.

7.4 Protecting e-commerce system

Securing your e-commerce system

With this high level of dependency upon the services provided by e-commerce systems, it is essential that they are protected from the threats posed by hackers, viruses, fraud and denial-of-service (dos) attacks.

Identifying e-commerce threats and vulnerabilities

- ***Types of threats***
- Hackers attempting to penetrate a system to read or alter sensitive data.
- Burglars stealing a server or laptop that has unprotected sensitive data on its disk. Imposters masquerading as legitimate users and even creating a website similar to yours
- Authorized users downloading a web page or receiving an email with hidden active content that attacks your systems or sends sensitive information to unauthorized people.
- Where (or who) are the potential sources of threats?
- What level of expertise is the hacker likely to possess? How much effort are they likely to expand in attempting to breach your security? • What facilities and tools are available to them?

Risk assessment

A risk assessment can be carried out to provide an organization with a clear understanding of the risks facing its e-commerce system and associated business processes, and the potential impact if a security incident arises.

7.5 Common E-commerce Security Tools

❖**Authentication**

Several techniques that can identify and verify someone seeking to access an ecommerce system.

- ✓ a user name and password combination, where the password can vary in length and include numbers and characters.
- ✓ ―two-factor‖ authentication requiring something the user has(egan authentication token) and something the user knows(eg a personal identification number).
- ✓ A digital certificate that enables authentication through the use of an individual‘s unique signing key.
- ✓ A person‘s unique physical attribute, referred to as a biometric. This can range from a fingerprint or iris scan, through to retina or facial-feature recognition.

❖**Access control**

- ✓ Network restriction to prevent access to other computer systems and networks

- ✓ Application controls to ensure individuals are limited in the data or service they can access
- ✓ Changes to access privileges must be controlled to prevent users retaining them if they transfer between departments or leave the business.

❖**Encryption**

Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties.

❖**Firewall**

A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules.

Firewall typically takes one of two forms:

Software firewall:-

Specializedsoftware running on an individual computer, or

Network firewall:-

A dedicated device designed to protect one or more computers.

Types of firewalls

- Whether the communication is being done between a single node and the network, or between two or more networks.
- Whether the communication is intercepted at the network layer, or at the application layer.
- Whether the communication state is being tracked at the firewall or not.

With regard to the scope of filtered communication there exist:

- **Personalfirewalls,** a software application, which normally filters traffic entering, or leaving a single computer.
- **Network firewalls,** normally running on a dedicated network device or computers positioned on the boundary of two or more networks. Such a firewall filters all traffic entering or leaving the connected networks.

❖**Intrusion detection**

The software related to intrusion detection monitor system and network activity to spot any attempt being made to gain access. If a detection system suspects an attack, it can generate an alarm, such as an e-mail alert, based upon the type of activity it has identified.

Preventing problems from viruses, Trojans and worms Anti-virus software

There are different types of anti-virus software:

- ***Virus scanners:***-must be updated regularly, usually by connecting to the supplier‘s website, in order to recognize new viruses.
- ***Heuristics software:***- detects viruses by applying general rules about what viruses look like, while it does not require frequent updates, this software can be prone to giving false alarms.

The threat of virus infection can be minimized by:

- Using a virus checker on your internet connection to trap viruses both entering and leaving he business it systems.

- Running virus checkers on servers to trap any viruses that have managed to evade the above check.
- Running individuals virus checkers on users pc‘s to ensure the they have not down loaded a virus directly of inadvertently introduced one via a cd of floppy disk.

Other methods of preventing viruses;

- Installing software patches provided by the supplier of your operating system to close security loopholes that could be exploited by viruses.
- Using a firewall to prevent unauthorized access to your network.
- Avoiding download of unauthorized programs and documents from the internet and ensuring your staff adhere to this policy.

❖**Digital identity**

Digital entity is the electronic representation of a real-world entity. The term is usually taken to mean the online equivalent of an individual human being, which participates in electronic transaction on behalf of the person in question.

Digital identity refers to the aspect of digital technology that is concerned with the meditation of people‘s experience of their own identity and the identity of other people and things.

The basis of digital identity:-

- is the online presence of an individual or business...gives access to online services – authentication
- defines the level of access to online services-authorizationis a repository of
- information for use by the subscriber, for the subscriber.. is the first point of all online communications.

7.6 Client server Network security

Client server network security is the main problem for system administrators faces as they the opposing goals users‘ maneuverability and easy access, site security and confidentiality of local information.

A system that records al log can alert managers to the need for stronger measures. Where secrets are at stake or where important corporate assets must be made available to remote users, additional measures must be taken hackers can use password guessing, password tapping, security holes in programs, or common network access producers to impersonate users and thus pose a treat to server.

Client server network security problems are:

- Physical security holes result when individuals gain unauthorized physical access to a computer.
- Software security holds result when badly written program or privileged software are compromised into doing things they should not.
- Inconsistent usage holes result when a system administration enables a combination of hardware and software such that the system is seriously flawed from security point of view the incompatibility of attempting two unconnected but useful things creates the

security hole. Problems like this are difficult to isolate once the system is set up and running, so it is better to carefully build the system with them in mind.

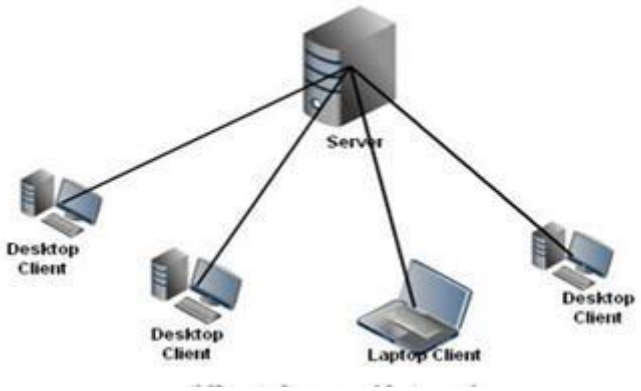


Fig.7.1.Client/server network functional diagram

Several protection methods have been developed including:

- Trust based security
- Security through obscurity
- Firewall & network security

➢**Trust based security**

Trust based security means to trust every one and do nothing extra for nothing. It is possible not to provide access restriction of any kind and to assume that all users are trustworthy and competent in their use of the shared network.

➢**Security through obscurity**

Security through obscurity (STO) means any network cab be secure as long as nobody outside it‘s management group is provided information on a need to know basis.

➢**Firewall & network security**

A firewall between the corporate network and outside world. The term firewall can mean many things to many people but basically it is a method of placing a device a computer or a router between the network and the internet to control and monitor all traffic between the outside world and the local network. The device allows insiders to have full access to service on the outside while grating access from the outside only selectively base on log –name, password, IP address or other identifiers.

7.7 Data and Message Security

Encryption

The process of encoding plain text messages into cipher text message called as **encryption**. The reverse process of transforming cipher text message back to plain text is called **decryption**. Decryption is exactly opposite of encryption.

Encryption transforms a plain text message into cipher text, where as decryption transforms a cipher text message back into plain text. The encryption process takes place

through the use of algorithms, complex mathematical functions that are applied to the message and make it unreadable without the decryption key.

Encryption technology can help in other ways such as:

- By establishing identity of users
- Control the unauthorized transmission or forwarding of data
- Verify the integrity of the data
- Ensure that user take responsibility for data that have transmitted
- It can be used either to keep communication secret or to identify people involved in communications.

E-commerce system can use three types of encryption technique:

- Public key encryption or asymmetric key-based algorithm
- Symmetric key-based algorithm or block and stream ciphers
- Hashing or creating a digital summery of a string or a file **Public key encryption or asymmetric key-based algorithm:**

This method uses one key to encrypt data and a different key to decry the same data.

Symmetric key-based algorithm or block and stream ciphers:

Using these cipher types data is separated into chunks, and those chunks are encrypted and decrypted based on a specific key. Stream ciphers are used more predominantly than block ciphers, as the chunks are encrypted on a bit-by-bit basis. This process is much smaller and faster than encrypting larger chunks of data.

Hashing or creating a digital summery of a string or a file :

This is most common way to store password on a system, as the password are not really what's stored , just a hash that cannot be decrypted.

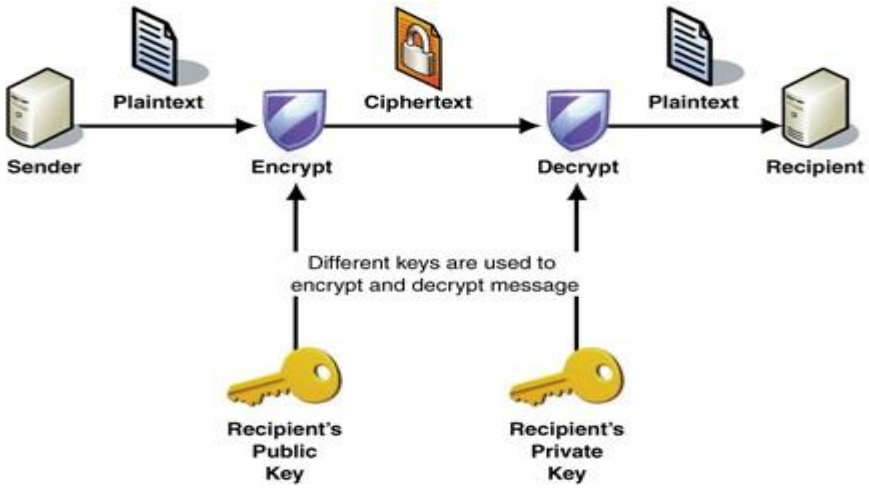


Fig. 7.2. Encryption