E-commerce

FOR DIPLOMA STUDENTS
Lecture Notes Prepared
by

BARSHA RANI PATEL

IT Dept.

JHARSUGUDA ENGINEERING SCHOOL, JHARSUGUDA

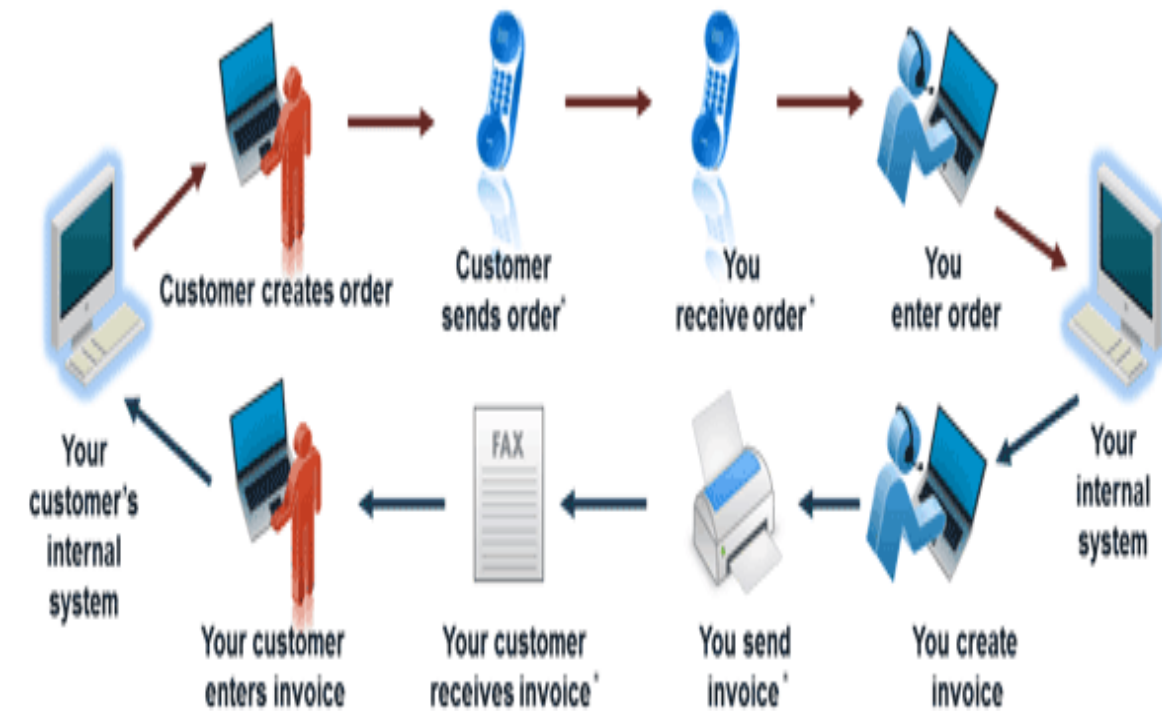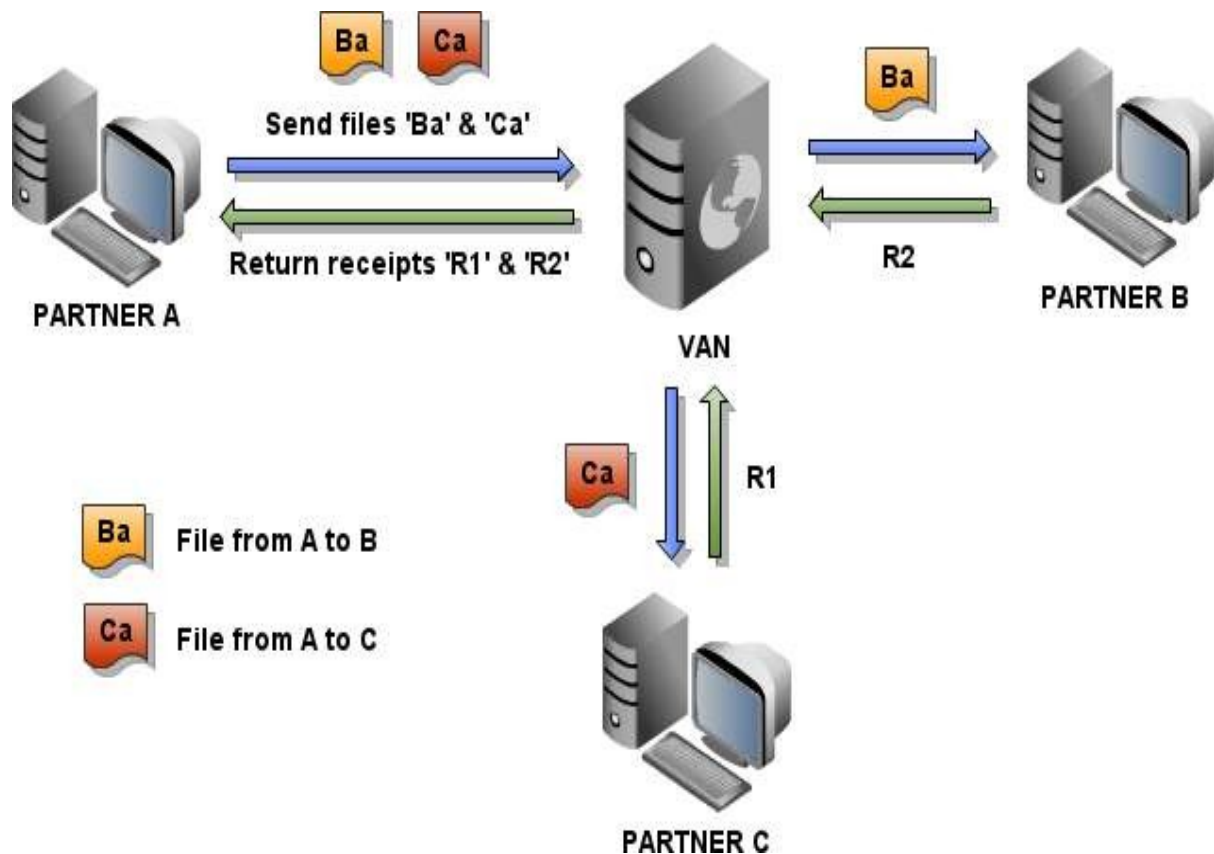# UNIT - 1

E-commerce

Content

1. Introduction of E-commerce
2. Defination
3. Features
4. Traditional commerce v/s E-commerce

Introduction of E-commerce

E-commerce was first introduced in the 1960s via an electronic data interchange (EDI) on value-added networks (VANs). The medium grew with the increased availability of Internet access and the advent of popular online sellers in the 1990s and early 2000s.

Send files 'Ba' & 'Ca'

Return receipts 'R1' & 'R2'

PARTNER A

VAN

PARTNER B

R2

R1

Ca

PARTNER C

Ba File from A to B

Ca File from A to C

Defination

E-commerce or electronic commerce is a process of buying and selling of goods and/or services via electronic channels such as the Internet to reduce cost, improve the quality of goods and services while increasing the speed of delivery. E-commerce refers to paperless exchange of buisness information using following ways

1. Electronic data Exchange

2. Electronic Mail (Email, Fax)

3. EFT

4. Other network based technologies

Features

1. Non-cash payment

2. 24*7 service availability

3. Advertising /marketing

4. Improved sales

5. Support (pre sales and post sales)

6. Inventory Management

Traditional Commerce V/S E-commerce

S.No.	TRADITIONAL COMMERCE	E-COMMERCE
1	Traditional commerce refers to the commercial transactions or exchange of information, buying or selling product/services from person to person without use of internet.	E-commerce refers to the commercial transactions or exchange of information, buying or selling product/services electronically with the help of internet.
2	In traditional commerce it is difficult to establish and maintain standard practices.	In traditional commerce it is easy to establish and maintain standard practices.
3	In traditional commerce direct interaction through seller and buyer is present.	In traditional commerce indirect interaction through seller and buyer occurs using electronic medium and internet.
4	Traditional commerce is carried out by face to face, telephone lines or mail systems.	E-commerce is carried out by internet or other network communication technology.
5	In traditional commerce processing of transaction is manual.	In e-commerce processing of transaction is automatic.
6	In traditional commerce delivery of goods is instant.	In e-commerce delivery of goods takes time.
7	Its accessibility is for limited time in a day.	Its accessibility is 24×7×365 means round the clock.
8	Traditional commerce is done where digital network is not reachable.	E-commerce is used to save valuable time and money.

9	Its resource focuses on supply side.	Its resource focuses on demand side.
10	In traditional commerce customers can inspect products physically before purchase.	In e-commerce customers can not inspect products physically before purchase.
11	Its business scope of business is a limited physical area.	Its business scope is worldwide as it is done through digital medium.
12	For customer support, information exchange there is no such uniform platform.	For customer support, information exchange there is exists uniform platform.

Activities of e-commerce

Contents

1. Providing Customer Services
2. Communication Within the Organization
3. Gathering Information
4. Publishing And Distributing

Providing Customer Services

1. Provide as much Information as Possible

2. Always send confirmation emails

3. Track orders carefully.

4. Respond to emails and calls as quickly as possible

5. Make customers feel important

6. Setup a live chat

7. Make it easy to buy

8. Provide multiple payment options

9. Have a help link prominently displayed

Communication Within the Organization

In the development of an organizational structure, communication channels are an important consideration. The manager in a hierarchical system becomes a link in the communication chain. It is the hierarchical system that gives direction to and imposes restrictions upon the flow of communications. Management decisions and directions flow from higher to lower levels in the organization. Responses and reports from the lowerlevel managers flow upward in the organization.

Committees influence the communication process within an organization. A well-run committee can serve as a supplementary link in the communication chain and provide a means for disseminating information.

The Communication Process

To set the stage for information and message flow through an organization, let's review the basic elements of the communication process. These elements include: someone to send the message (the encoder), some means for channeling it, someone to receive it (the decoder), and a feedback mechanism.


Regardless of the source, the message passes through the sender's filter before it reaches the intended recipient. The sender injects his attitudes and perceptions into the message; determines who should receive it; and the channels through which it should flow, i.e., upward, down-ward, laterally, or a combination of these.

The Communication Channels

The communication channel selected for transmitting a message plays a significant role in maintaining the quality of the original message in its passage from the sender to receiver.

Considering the possible barriers, the sender must choose the channel which he feels will best guarantee transfer of the essence and meaning of his message without misunderstanding or distortion. To provide repetition, the message must be transmitted through more than one channel, as in spoken and written form, or transmitted more than once through the same
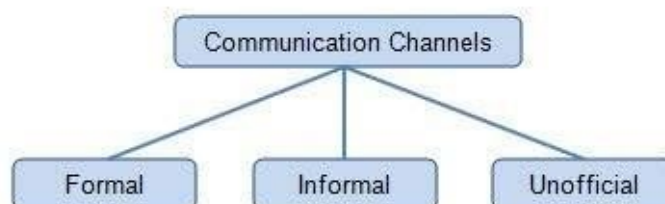

channel, as in TV advertising.

1. Formal. The communication within the formal organizational structure that transmits goals, policies, procedures, and directions.

2. Informal. The communication outside the formal organizational structure that fills the organizational gaps, maintains the linkages, and handles the one-time situations.

3. Unofficial. The interpersonal communication within (or among) the social structure of the organization that serves as the vehicle for casual interpersonal exchanges, and transmittal of unofficial communications

Gathering Information
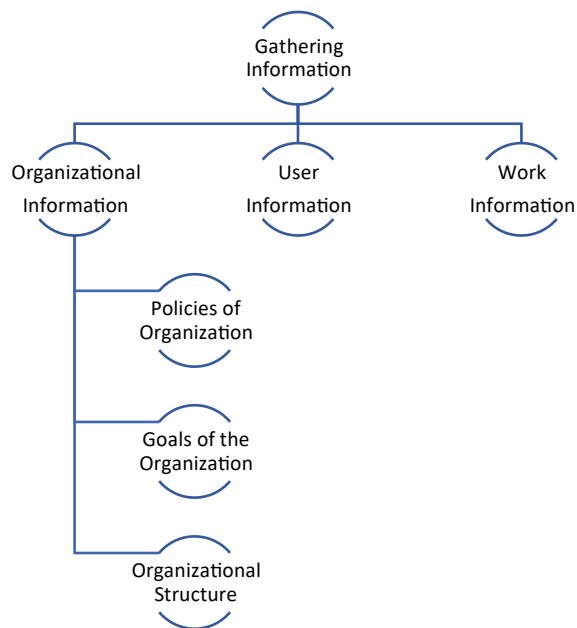
Publishing and Distributing

Information Management systems (MIS)-a computer-based system that provides info and support for effective managerial decision making.
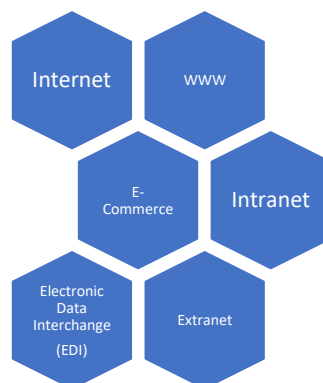
Goals of E-commerce

Contents

Introduction

As already defined, e-commerce is a modern business methodology which addresses the needs of the organisations, merchants and consumers to cut costs while improving the quality of goods and services. Actually, the goals of e-commerce are not only important for start-up business but also for every e-business who want to see their business prosper in the sense of money or popularity.

Objectives

1. <u>Customer Experience -</u> Customer's feedback is the most important goal of e-commerce. Since, the profit of a e-business wholly depends on the customer's satisfaction. Therefore, customer the journey from the time of searching or ordering a product to its delivery, each step must satisfy the customer's requirement and basing on the customer's rating, the company must focus for developing that particular weak area.

2. <u>Transaction Devices</u> - In today's world, the shopping and other similar services have become online, hence cash payment transaction have become obsolete, as they involve a lot of time and people. In order to save time, e-commerce must set up a goal to reduce the time and people involved to settle the financial transaction between the buyer and the seller. So, setting up payment systems or transaction devices has become one of the most crucial goals of e-commerce.

3. <u>Ease of Moving from Legacy Systems -</u> User requirements are a major concern as they keep changing from time to time. E-commerce websites must have their interfaces and services updated according to the user requirements that come each time. As the services and user requirements keep changing rapidly in today's world, ease of moving from legacy systems is an important goal of e-commerce.

4. <u>Lower Product Cycle Time -</u> A business organisation has a lot of work in management of product cycle as it has a lot of products that it needs to sell. E-commerce applications were introduced to lower the work load of both seller and the customer. The workload can be lowered in one of the major things, i.e., product cycle is maintained properly without spending a lot of money and people. Involving people even slows things a lot which can cost a lot to the organisation. So, the product cycle time must be lowered.

5. <u>New revenue collecting techniques -</u> E-commerce impacts the revenue cycle largely in two ways, by changing how the business sells it is product and how the business collects its payment. E-commerce was introduced to lighten these loads by making the online services and new techniques for easy maintenance.

6. <u>Not Bounded By Limitations -</u> E-commerce should not be restricted by any barriers like any bricks-n-mortar retailer that have to take prior permissions from municipality corporation, or they have to check which products the retailer should sell in their locality. So likewise, e-commerce business shouldn't have any type of barriers rather it should be free from barriers.

7. <u>Security -</u> Security means setting authorised access boundary for the protection of a system against any outsider. E-commerce involves business. Business involves a large organization that has a lot of data of its products, its customers information, payment and transaction information and various other sensitive data which when exposed can put the business as well as the customers in grave danger. So, e-commerce application must set up a goal of providing security.

8. <u>Wider Reach -</u> Unlike bricks-and-mortar retailers that can do its business only within a boundary like a country or a state or within a particular region, e-commerce websites help the online sellers to reach people and do its business worldwide. So, e-commerce business should be expanded worldwide for doing profit making business and this must be a goal of e-commerce.

Summary

1. Customer's feedback is the most important goal of e-commerce. The company must focus on customer's feedback for developing that particular weak area.

2. Setting up payment systems or transaction devices has become one of the most crucial goals of e-commerce. cash payment transaction has become obsolete, as they involve a lot of time and people.

3. As the services and user requirements keep changing rapidly in today's world, ease of moving from legacy systems is an important goal of e-commerce.

4. The product cycle time must be lowered, in order to reduce time and labour.

5. E-commerce was introduced to lighten the loads of revenue collecting by making the online services and new techniques for easy maintenance.

6. E-commerce business shouldn't have any type of barriers rather it should be free from barriers.

7. E-commerce application must set up a goal of providing security in order to protect various information regarding customer, payment and transaction etc.

8. E-commerce business should be expanded worldwide for making profit rather than concentrating on one area.

Functions of E-commerce

Every business, regardless of its size and flexibilities must perform four basic functions to succeed.

The basic functions of E-Commerce

1. Communication function
2. Process management function
3. Service management function
4. Transaction capabilities

Communication Function

The communication function is aimed at the delivery of information and/or documents to facilitates business transactions.
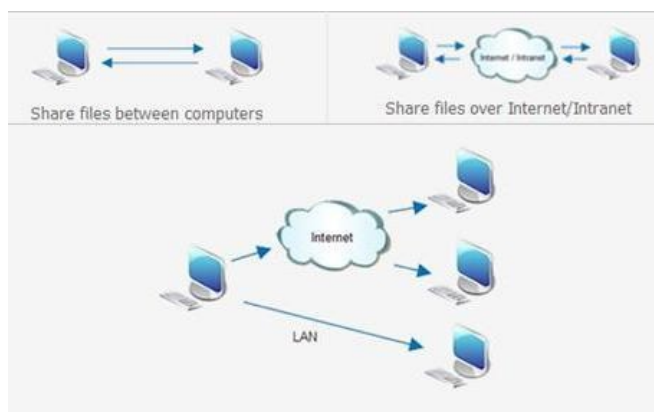
For example: E-mail

Process Management Function

The process management function covers the automation and improvement of business processes.

For example: Networking two computers together so that they can share and transfer data rather than have a person to take data from one computer to another.

Service Management Function

Application of technology to improve the quality of service.

Example: Federal Express website.

It permits customers to track shipments and the schedule picks up 24 hours a day with a worldwide network (without having to talk to a service representative).

Customer service is greatly enhanced due to the site's capabilities.

Transaction Capabilities

Provides the ability to buy/sell on the Internet or some other online service.

Example: Retail websites of Amazon.com and Olx.com

Advantages and Limitations of E-commerce

Contents

1. 1.Introduction
2. 2.Advantages
3. 3.Limitations

Introduction

Electronic commerce, commonly written as e-commerce, is the trading or facilitation of trading in products or services using computer networks, such as the Internet. It is now available everywhere at anytime. Whenever we open the net, we see the attractive banner advertisement that invites us to its websites and tries to tell us about its products or services. The encircled part given here is an example of an advertisement that we get when we open an website.

Advantages of E-Commerce

1.Economy - E-commerce is highly economical. Unlike the showrooms or shops, in e-commerce there is no physical existence or store space, insurance or infrastructure investment. All we need is just an idea to sell a unique product and a well designed website to reach the customers and a partner to do fulfilment.

2.Lower Cost - E-commerce on internet is extremely cost effective. It reduces logistical problems and puts a small business on a par with giants like flipkart, amazon, jabong etc. e.g.-a over-the-counter transaction cost Rs52, while in net the same transaction cost 1 rupee. The sooner it makes the transaction, the more cost-effective the transaction becomes.

3.Better Customer service - E-commerce focuses on better and quicker customer service. e.g. The overnight package delivery service, where tracking numbers allow customers to check the whereabouts of a package online. We can access our personal account directly over the net, rather than calling the company waiting for a clerk who taps into your account.

4.Greater Profit Margin - E-commerce means greater profit margins. E.g. The cost of processing a conventional airline ticket is Rs. 400. According to one travel agency, processing the same ticket over the web is Rs. 50 only.

5.Knowledge Markets - E-commerce helps to create knowledge markets. Small groups inside big firms can be funded with seed money to develop new ideas. E.g. The flipkart has gives a team to submit the order history report of each and every transaction made throughout the year. So, for that, it invests the money for the small group to carry out the project.

6.Swapping goods and services - It refers to the barter system through web, e.g. WebSwap, BarterTrust.com etc. E.g. an employee of a product based company offers his cell phone and in exchange he gets a cell phone of the latest version (conditions apply - within six months of buying of the old cell phone).

7.Information Sharing, Convenience, and control - E-commerce improve information sharing between merchants and customers and promote quick, just-in-time deliveries. They both save money, are online 24 hrs. a day, 7days a week thereby experiencing no traffic jams, no crowds and do not have to carry heavy shopping bags.

Control is an another aspect. For example, instead of bank controlling the relationships with the customer, customer today can have much more control of their banking needs through web sites. E.g. SBI provides net-banking.

8.Quick comparison shopping - E-Commerce helps customers to compare and contrast between the various products of same type and then choose what is suitable for them. Various retailers use common E-Commerce websites, example Flipkart, to sell their products. These E-Commerce websites make a brief comparison between the products of these retailers (look, type, price, availability, offers etc.) and provide them to the users so that the users can make a choice on their own without taking the trouble of doing that themselves and purchase the products as they want. So, e-commerce websites are widely useful.

9.Teamwork - E-commerce helps people work together. E-mail is one such example, by which people cooperate with each other to exchange information and work on solutions. It has changed the way organisation communicate with suppliers, vendors, business partners and the most important customers. More communication means better overall results.

10.Productivity Gains - E-Commerce means productivity gains. Using the web technology as a medium of product management has led to an improved productivity.

11.Customization - Digital products are highly customizable. They are easy to reorganise ,revise, or edit. With information about consumer tastes and preferences, products can be differentiated (customized) and matched to individual needs.

12.Ensure Secrecy - EC devices have in built security measures. E.g. password, cipher etc. are some of the measures which provide security and prevent unauthorised access and use of data, information and transaction.

Limitations

1. High risk of Internet start-up Organizations - Many stories unfolded in 1999 about successful executives in established firms leaving for internet start-ups, only to find out that their "get rich" dream with a dot.com was just that a dream. However, many dot.com organizations bubble bursted in 2000 and onward due to various reasons like lack of good revenue model, everything is not possible through dot.com, problem related to customer satisfaction etc.

2. Lack of a blueprint for handling E-commerce - There is continuing shortage of e-literate people in the workplace. In a survey published in "Computerworld", nearly nine out of 10 respondents said only a few of their key managers have e-commerce skills, internet skills, internet experience and foresight.

3. E-commerce is not free - So far, success stories in e-commerce have favored large business with deep pockets and good funding. According to recent reports, small retailers that go head-to-head with e-commerce giants are fighting a losing battle. They simply cannot compete on price or product offering.

4. Security - Security can be a problem for online business. In 2000 Economist article,95 percent of Americans expressed reluctance to give out their credit card numbers via the Internet. For millions of potential cyber customers, the fear of credit card theft is a real one. Consumers have to feel confident about the integrity of the process before they commit to the process.

5. Customer relations problems - There can be lack of system security, reliability or standards owing to poor implementation of e-commerce. Not many business realize that even an e-business cannot survive over the long term without loyal customers.

6. System and Data Integrity - data protection and the integrity of the system that handles the data are serious concerns. Computer viruses are rampant with new viruses discovered everyday. Viruses cause unnecessary delays, file backups, storage problems, etc. The danger of hackers accessing to files and corrupting accounts adds more stress to an already complex operation.

7. **Products People Won't Buy Online** - "Product/market fit means being in a good market with a product that can satisfy that market." Imagine a website called furniture.com, where venture capitalists are investing millions in selling home furnishings online.

In this case of a sofa, you would want o sit on it, feel the texture of the fabric etc. Beside the "sofa test" factor, online furniture stores face costly returns, and the kinds of delivers that cannot be expedited.

8. Corporate Vulnerability - The availability of Product details, catalogs, and other information about a business through its website makes it vulnerable to access by the competition. The idea of extracting business intelligence from the competition Web pages is called Web farming, a term coined by Richard Hackathorn.

9. Fulfillment problems -Tales of shipping delays, websites crashing under pressure continue to be a problem in e-tailing. Customer confidence in a e-commerce's ability to deliver during

heavy shopping seasons continues to be a headache. Even happy customers say the experience could be improved.

10. System scalability -A business develops an interactive interface with customers via a website. After a while, statistical analysis determines whether visitors to the sites are one time or recurring customers. If the company expects 2 million customers and 6 million show up, website performance is bound to experience degradation, slowdown and eventually loss of customers. To keep this problem from happening, a website must be scalable, or upgradable on a regular basis.

11. Consumer Search is not efficient or Cost-Effective - On the surface, electronic marketplace appears to be a perfect market, where worldwide sellers and buyers share information and trade without intermediaries. However, a closer look indicates that new types of intermediaries are essential to e-commerce. All these intermediaries are added to transaction costs.

Summary

1. E-Commerce is a method of trading various products online, using the technology of internet, and is available worldwide these days.
2. E-Commerce is economical in various ways and makes lower costs for products compared to the one in the market.

3. E-Commerce provides better customer services and a good knowledge market for its own

4. development and working team.
5. E-Commerce provides a better product exchanging way by the help of comparison shopping, information sharing between merchants and customers and better teamwork by making partnership with other sources.

6. E-Commerce, most importantly, provides a confidentiality between the customers by ensuring secrecy.

7. E-Commerce products are customizable and the productivity gain is higher.

8. E-Commerce has a number of limitations as it has a lot of advantages.

9. E-Commerce has made many "get rich" dreams for startups taken aback.

10. E-Commerce requires some knowledges and skills which even today many don't possess.

11. E-Commerce sometimes makes a bad relation between customers and merchants taking the pricing problems, by making them higher.

12. E-Commerce is vulnerable to data loss when there are cheap and poor things used by the business merchants, resulting in degradation of the system and a huge loss of customers.

13. E-Commerce cannot sell everything (e.g. : furniture) online.

14. E-Commerce does not guarantee the safe delivery of products purchased online, which leads to fulfillment problems of the customer.

15. E-Commerce does not guarantee an efficient result of what the customer wants to buy.

Applications of E-commerce

Applications & Implementations

1. Document Automation in Supply Chain and Logistics

2. Domestic and International Payment Systems

3. News Groups

4. Enterprise Content Management

5. Online Banking

6. Online Shopping and Order Tracking

7. Instant Messaging

8. Online Office Suites

9. Social Networking

10. Electronic Tickets

11. Digital Wallet Management

12. Teleconferencing

1. Document Automation in Supply Chain & Logistics

- Supply chain - System of organizations, people, activities, info & resources in moving product or service from supplier to customer.

- Logistics - The commercial activity of transporting goods to customers .

- Document Automation - The design of systems and workflows that assist in the creation electronic documents .

- Supply chain and logistics involve online documents like invoice , packing slips / lists forms or reports of many types , which are usually the contracts between the consignee (buyer) and the consigner (seller) . It involves online services like user or seller registration , online document generator which generates these documents required . Hence , it is an implementation of e - commerce .

2. Domestic & International Payment Systems

- Payment System - System used to settle the financial transactions through the transfer of monetary value , and includes the institutions , instruments , people , rules , procedures , standards and technologies that make such exchanges possible.

- Electronic Payment can narrowly refer to e - commerce , as it is a payment made for buying and selling goods and services offered through internet .

- Domestic Payment refers to the payment made within the country and international payment refers to the payment made globally across various countries.

- International Payment refers to the payment made across the countries .

3. Newsgroups

- Newsgroups - It is a repository for messages posted from many users in different locations. These are functionally similar to the discussion forums on the World Wide Web .

- Newsgroup servers are hosted by various organizations and institutions . Most host their own servers or rent access to one , for their subscribers . It involves user subscription and payment online , it makes an important implementation of e - commerce .

4. Enterprise Content Management

- Enterprise Content Management (E C M) - It is a formalized means of organizing and storing an organization's documents , and other content , that relate to the organization's process .

- An organization has various branches worldwide which makes it a complex system to manage and hence keep it running . Thus , E C M was introduced which made the management online . E C M involves various document generation , transaction etc , online which makes it an important implementation of e - commerce .

5. Online Banking

- Online Banking - An electronic payment system that enables the customers of a bank or other financial institutions to conduct financial transactions through a website .

- Online Banking involves transactional and non - transactional activities . It has it's advantages to both bank and its customer . It allows them to permanently access the bank from anywhere in lower transaction costs and without any security problems .

- Since Online Banking involves online services and operations with the bank which is a major concept of e - commerce , so it is an implementation of e – commerce.

6. Online Shopping & Order Tracking

- online shopping - A form of e - commerce which allows the consumers to directly buy goods or services from a seller over the internet using any web - browser .
- order tracking - A process of determining the current and past locations of a unique item or property in distribution and logistics .
- Both online shopping and order tracking are e - commerce concepts by themselves . So they come under a crucial implementation of e - commerce .

7. Instant Messaging

- instant messaging - A type of online chat which offers real time text transmission over the internet .
- It provides online services to each and every user of the messaging application to communicate with the other users of the same application . This online service providing process is done using the e - commerce concepts , hence instant messaging is also an implementation of e - commerce .

8. Online Office Suites

- office suites - Offered by various websites in the form of *Software As A Service* . These can be accessed online by any internet - enabled device and allow people to work together world wide and at any time .
- Office Suites include various applications - Document Creation and Editing Applications , Publishing Applications , Collaborative Applications , and Management Applications .
- Office suites involve online services like document creating , editing and publishing services which can be made by a single person or a group of people from any location world wide . Since there is a trading of services using internet in office suites , it is an implementation of e - commerce .

9. Social Networking Services

- social network - A social structure made up of various individuals or organizations and other social interactions between these social actors .
- social networking service - It is a platform to build the social relations among people who share similar interests , activities , backgrounds , or real - life connections . It also represents each user's profile , social links and other additional services .
- Since it involves various online services to bring up individuals or organizations , or build various social interactions or relations between these social actors using the internet as a medium , it is an application of e - commerce .

10. Electronic Tickets

- ticket - It is a transit pass used to enter into a service or industry. It is mainly used in transport services or entertainment industry.
- electronic ticket - It is otherwise called as Digital Ticket. It is a more efficient method of ticket entry, processing and marketing for companies in the railways, flight and other transport and entertainment industries.
- It involves online registration services, online ticket booking services and payment system for purchasing the tickets. As a lot of online trading of products (tickets) and services are involved in electronic ticketing, hence it is an important implementation of   e - commerce.

11. Digital Wallet Management

- wallet - It is a small, flat case that is used to carry items such as cash, credit/debit cards, identification documents etc.
- digital wallet - It is an electronic device that allows the user to make e - commerce transactions.
- A digital wallet has both information and software component, in which it stores the complete information about the user/biller. It can be used anytime by the user to buy any product online from any e - commerce website, without any more form filling or identification documents.
- Since it involves online services like user registration services, online security services, online management services and online purchasing services, it is an important implementation of e - commerce.

12. Teleconferencing

- teleconference - Live exchange and mass articulation of information among several machines remote from one but linked by a telecommunication system.

- internet teleconferencing - It involves conducting a teleconference over the internet or a wide area network. It includes telephone conferencing, video conferencing and web conferencing.

- It involves various services, like online registration services and online teleconferencing services, provided by the various servers over the internet. So it is an implementation of e - commerce.

Summary

1. E - Commerce is the trading or facilitation of trading in products or services using computer networks , such as Internet .
2. E - Commerce has played a major role in the world since 1979 when Online Shopping was introduced .

3. Various applications of E - Commerce have been put to use in the society these days .

4. Various documents in logistics such as invoice , content lists , pick tickets , arrival acknowledgements or bill of landing are generated online in Supply Chain Management .

5. Online payment system is now - a - days the most common implementation of e - commerce.

6. Newsgroup subscription and services have been playing an important role in the society for online broadcasting of news worldwide , which has been one of the most successful implementations of e - commerce .

7. Management of multi - national organizations in world - wide have been dependent on online services like online documentation , collaboration , web content management , record management and business process management .

8. Online Banking involves various e - commercial methods of accessing the bank , such as registration of a new customer , checking the account balance or transferring funds , which are some services provided by the bank server over the internet .

9. E - Commerce itself is online shopping website or order tracking systems of a package .

10. Instant messaging has become one of the most common implementations of e - commerce where the clients use the service of messaging over the internet .

11. Online Office Suites are being used world wide , which have helped various people all over the world to work together .

12. Social Networking and Teleconferencing have been a benchmark in the society for making various social relations among people present all over the world .

13. People have been provided online services for generating electronic tickets for various official and entertainment purposes , which have been made cheaper than offline ticket counters .

14. Digital Wallets have done a much quicker services for purchasing goods and products over the internet from any e - commerce websites .

15. E - Commerce has changed the world in terms of providing goods and services .

E-Commerce - Business Models

E-commerce business models can generally be categorized into the following categories.

1. Business - to - Business (B2B)

2. Business - to - Consumer (B2C)

3. Consumer - to - Consumer (C2C)

4. Consumer - to - Business (C2B)

5. Business - to - Government (B2G)

6. Government - to - Business (G2B)

7. Government - to - Citizen (G2C)

8. Business-to-Administration (B2A)

9. Consumer-to-Administration (C2A)

10. Peer-to-Peer (P2P)

Business - to - Business

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to the final customer who comes to buy the product at one of its retail outlets.
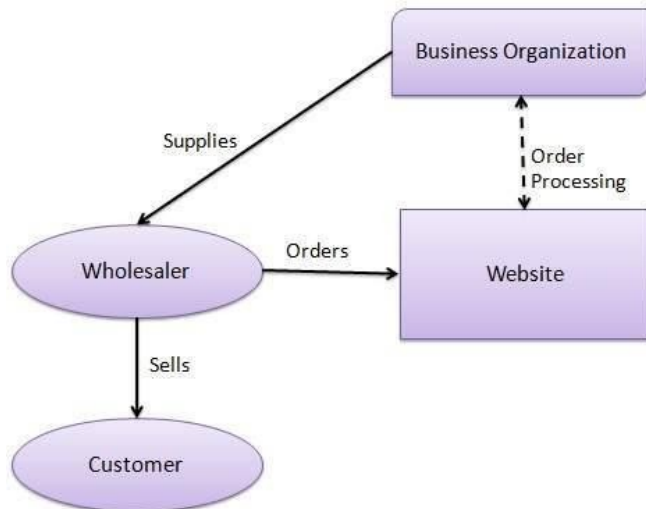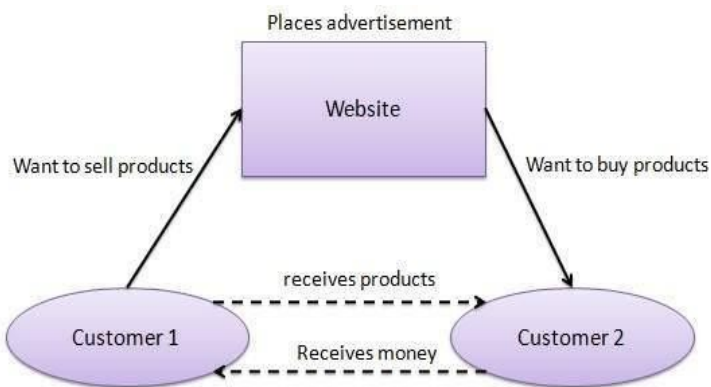

Business - to - Consumer

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.
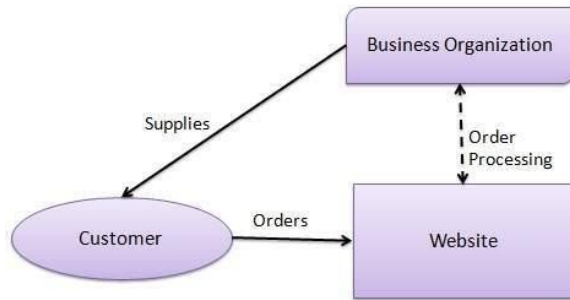
Consumer - to – Consumer

A website following the C2C business model helps consumers to sell their assets like residential property, cars, motorcycles, etc., or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Another consumer may opt to buy the product of the first customer by viewing the post/advertisement on the website.

Consumer - to - Business

In this model, a consumer approaches a website showing multiple business organizations for a particular service. The consumer places an estimate of amount he/she wants to spend for a particular service. For example, the comparison of interest rates of personal loan/car loan provided by various banks via websites. A business organization who fulfills the consumer's requirement within the specified budget, approaches the customer and provides its services.
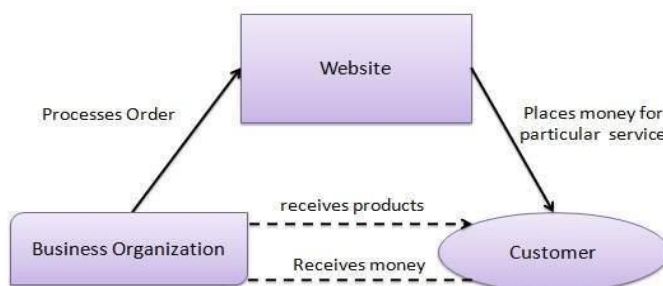
Business - to - Government

B2G model is a variant of B2B model. Such websites are used by governments to trade and exchange information with various business organizations. Such websites are accredited by the government and provide a medium to businesses to submit application forms to the government.

Government - to - Business

Governments use B2G model websites to approach business organizations. Such websites support auctions, tenders, and application submission functionalities.

Government - to - Citizen

Governments use G2C model websites to approach citizen in general. Such websites support auctions of vehicles, machinery, or any other material. Such website also provides services like registration for birth, marriage or death certificates. The main objective of G2C websites is to reduce the average time for fulfilling citizen's requests for various government services.

Business-to-Administration (B2A)

In this kind of eCommerce transaction, there are dealings between companies and public administration. It encompasses different services, such as social security, fiscal measures, legal documents, employment and so on.

Consumer-to-Administration (C2A)

In this eCommerce model, electronic transactions are carried between individuals and public administration. Some examples are distance learning, information sharing, electronic tax filing, and so on.

Peer To Peer (P2P)

Peer to peer, peer-to-peer or usually said as P2P, is a communications model in which each party has the same capabilities and either party can initiate a communication session.

This type that is a technology that helps their customers to share a computer resource and computer files to anyone they require without the need of a central web server.

In recent usage, peer-to-peer has come to describe applications in which users can use the internet to exchange files with each other directly or through a mediating server. In some cases, peer-to-peer communications is implemented by giving each communication node both server and client capabilities.

Those who are going to implement this model, both sides demand to install the expected software so that they could convey on the mutual platform.

This kind of e-commerce has very low revenue propagation as from the starting it has been tended to the release of use due to which it sometimes caught involved in cyber laws.

# UNIT – 2

Internet and www

What is the Internet?

- The Internet is a worldwide, publicly accessible series of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).
- It is a "network of networks" that consists of millions of --smaller domestic, academic, business, and government networks, which together carry various information and services, such as electronic mail, online chat, file transfer, and the interlinked web pages and other resources of the World Wide Web (WWW).
- The Internet and the World Wide Web are not synonymous.
- The Internet is a collection of interconnected *computer networks*, linked by copper wires, fiber-optic cables, wireless connections, etc.
- In contrast, the Web is a collection of interconnected documents and other *resources*, linked by hyperlinks and URLs(Universal Resource Locator).
- The World Wide Web is one of the services accessible via the Internet, along with various others including

1. e-mail, file sharing,

2. online gaming and

3. others described below

World Wide Web is an example of an information protocol/service that can be used to send and receive information over the Internet. It supports:

Multimedia Information (text, movies, pictures, sound, programs . . .).

Hypertext Information (information that contains links to other information resources)

Graphic User Interface (so users can point and click to request information instead of typing in text commands).
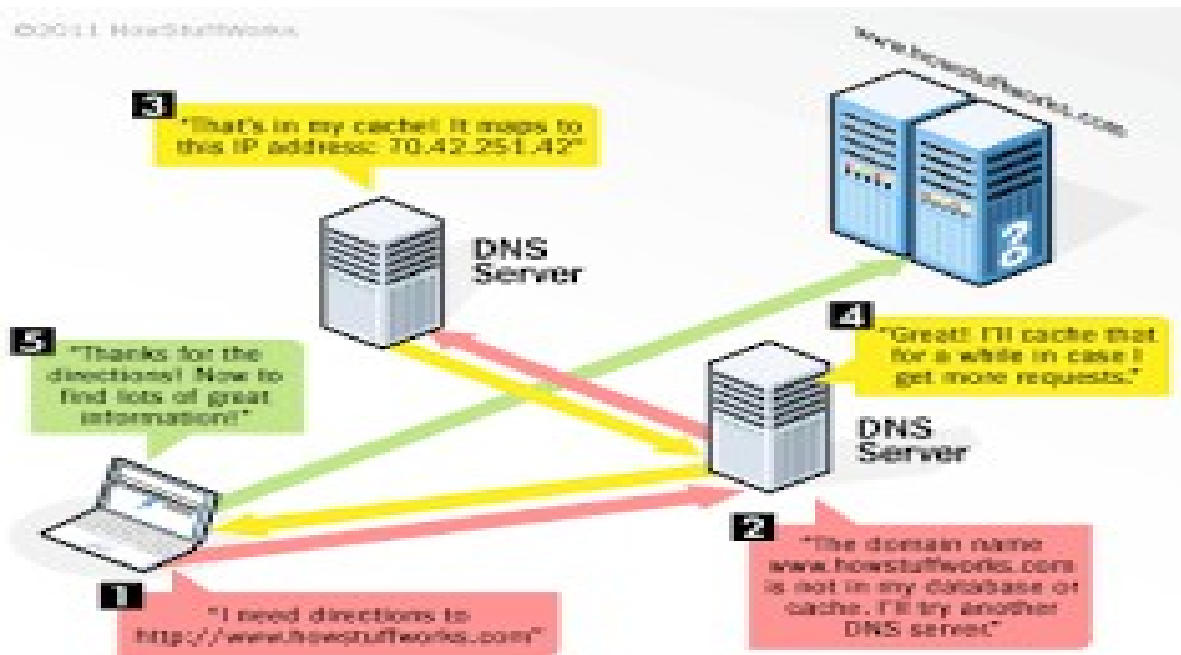
Domain Name system

It is a hierarchal distributed naming system for computers, services or any resource connected to the internet.

It associates various information with domain names associated to each of the particular entities.
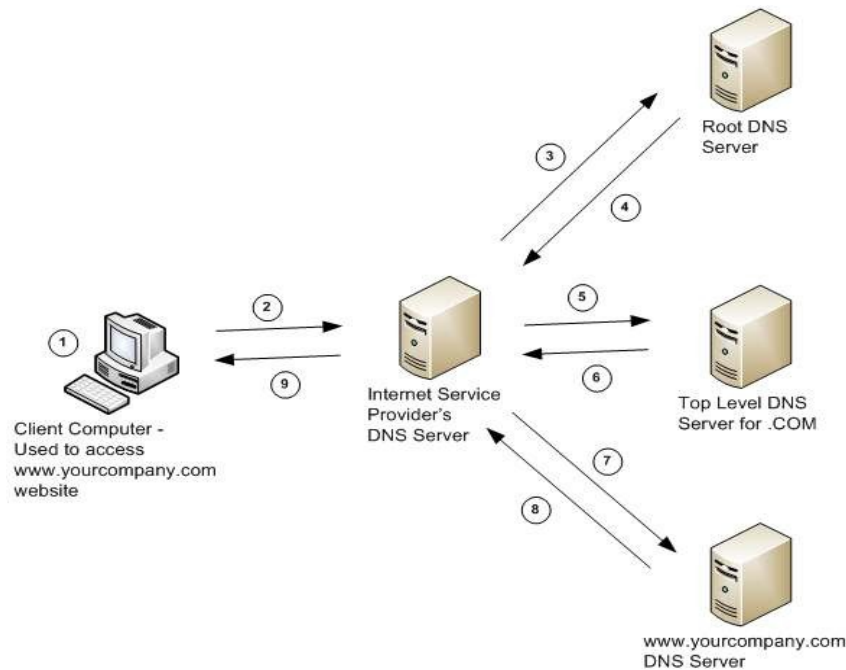
Domain Name

Definition

- It is a sequence of alphanumeric labels separated by dots read left to right. They are read from node up to the root. They are maximum 255 characters in length. Each domain name has an IP address attached to it . For e.g. www.example.com has an address 64.236.29.119 .
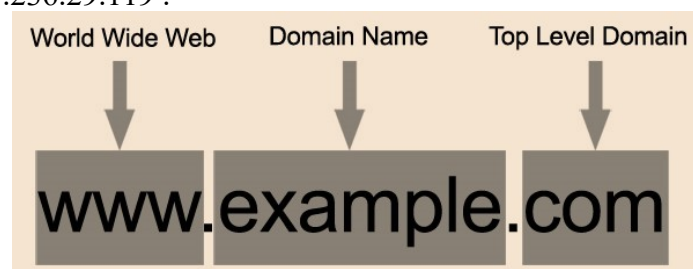
Functions of DNS

- It translates the domain to numerical IP addresses needed for the purpose of locating and identifying computer services and devinames ces with the network protocols. For e.g. ip address of www.google.com is 64.233.160.0
- It quickly updates itself allowing the service location on the network to change without affecting the end users who continue to use the same hostname.

- It assigns the domain names and maps the names on the internet resources by designing authorative name servers for each domain.

Classification of DNS

The domain name space is divided into different levels according to the hierarchical structure as designed by ICANN (Internet Corporation for Assigned Names and Numbers)

1. Top level domain: These are the highest level of domain names mentioned at the far right of any domain name. For e.g. .com, .org etc. .
2. Second level and other lower level domain: These are domains mentioned to the left of top level domain name. For e.g .co.in .
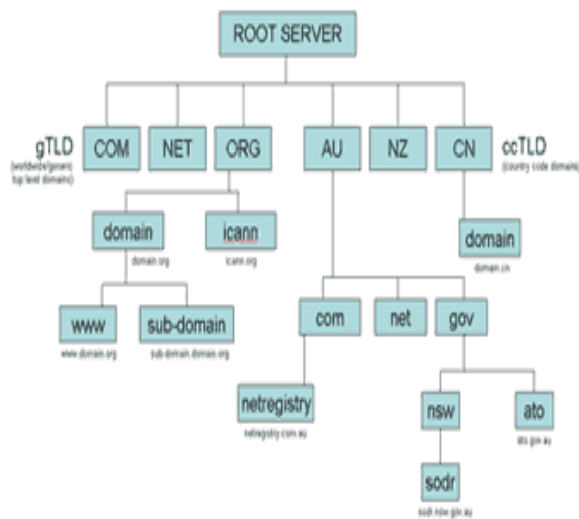
Types of TLDs in the internet

The Internet Assigned Numbers Authority(IANA) has classified various TLDs into four main categories as follows:

1. Infrastructure TLDs: These were original TLDs specific to particular agencies like ARPA(Advanced Research Projects Agency).
2. Generic TLDs(gTLDs):These are registered hosts according to the type of use. For e.g. .com, .org etc..
3. Sponsored TLDs(sTLDs): These are registered hosts sponsored by various companies. For e.g. .android ,.axa ,.cern.
4. Country code TLDs(ccTLDs): These are used for sites belonging to a particular country. For e.g. .in(India),.au(Australia).

Name	Entity type	Administrator	Use
.com	commercial	Verisign	For profit oriented business entities
.org	organization	Public Interest Registry	For non profit organizations
.net	network	Verisign	For network of systems or sites that are portal to smaller websites
.int	International organizations	IANA	For organizations endorsed by a treaty between nations
.edu	Higher education esp. in US	Educause(via Verisign)	For educational institutions only

Types of TLDs in the internet

Importance of domain names in e-commerce

1. Strong Domain Names: As there are millions of domain names, a short memorable domain name may be lost in the cyberspace.So domain names must be strong enough to create a successful presence online.
2. Improved credibility and visibility: It means to deserve our customers trust we need a short descriptive and easy to remember domain name. It gives customers an easy way to find and remember us.
3. Mobility: Once we have got our main domain name, then we need to buy other top level domains to expand our business as having local TLDs makes local customers more likely to trust.
4. Search result rankings :The domain name plays an important role in search engine ranking. For e.g. .com receives more importance than .co.in now a days.
5. Choosing the right domain: For business ,choosing the right domain is a key to success. If the domain name matches your company name, it reinforces your brand .Customers can remember it and can pass it on to their friends. It generates traffic to our website and builds reputation.

Problems faced while using TLDs

- Increase in fake websites thus leading to difficulty in choosing the proper website.

- Advertisements in the internet result in redirecting the host user to anonymous and unauthenticated sources or websites.

- Rise in vulnerability issues like crash of domain name servers by malicious users due to which various proper websites are not found.

- Now a days buying a registered domain is expensive.

Types of networks, Internet service provider, WWW,

Internet and Extranet

Contents

Types Of Networks

1. Local Area Network
- LAN are a group of micro-computers or terminals located in the same general area and connected by a common cable (communication circuit) so that they can exchange information.
- E.g., They are typically used within the same building or a set of building situated in a close area.
- These are generally privately owned.

Uses of LAN

1. To share the resources between PCs and workstations.
2. To use only one type of transmission medium (mostly bus, ring, star).
3. They have low delay and make very few errors.

2. Metropolitan Area Network
- MAN is a network covering a large geographical area that usually surrounds a city or country area, connecting various buildings or other facilities of private or public within this city wide area.
- This can support both data and voice, and might even be related to the local cable TV network.
- Many telephone companies provide a MAN service called switched multi-megabyte data services.

3. Wide Area Network
- WAN covers a large geographical area, often a country or continent and are called remote networks. Its nodes (micro-computers) can surround cities, states, or even national boundaries.
- This network interconnects computers, LANs, BNs, MANs and other transmission facilities on a countrywide or worldwide basis.
- It provides long distances transmissions of data, voice, image and video info over large areas.

- WAN are created using specially conditioned telephone lines, satellite data transmission.
- There are 2 types of WAN:

1. Hierarchical networks
2. Distributed data processing networks

4. Backbone Network (BN) or Campus Area Network (CAN)
- Here, a large central networks that connect all the terminals, micro-computers, main frames, local area networks that connect all the terminals, micro-computers, main frames, LAN and other communication equipment on a single company or university site, It is also known as campus area network (CAN).

5. Business Area Network
- BAN is the network infrastructure that is used to interconnect business within a multi-tenant building, business park or campus.
- It leverages the public MAN or WAN for connectivity between the BAN and to the business Tenant Services (BTS) provider's point-of-Presence (PO).

Internet Service Providers

Definition

- Company that has a connection to the internet and charges the public a fee to use part of that connection.

Functions

- Sell connections to the internet.
- Deliver a wide range of services to individual users and organizations.

Objectives in Choosing an ISP

- Should be decided on the nearness to a backbone.
- Service provider's ability to continue delivering services in the face of internal/external system and connective failures.
- Provider should have more than one connection for routing traffic to the internet.
- Should have internal system redundancy.

Different tires of ISP
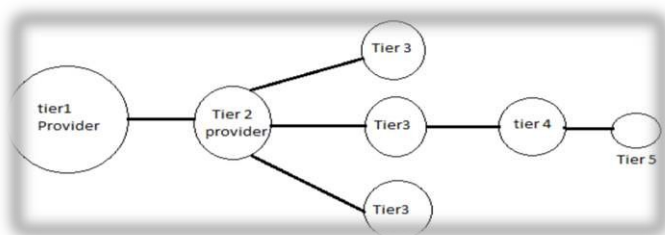
WWW (World Wide Web)

- World Wide Web is a storehouse of information spread all over the world and linked together.
- It uses the concept of hypertext.
- Information is stored in documents.
- It is a series of interconnected documents.
- Pointer concept is used.
- Hypertext on the web is known as page and main page is called as a home page.
- After establishing a web hosting arrangement with ISP (internet service provider), it allocates storage   space which will be accessed each time a request comes in.
- Mostly web pages uses the language of HTML.
- Information on any subject can be of 2 types :-

i) Undistributed – whole information may consist one or more web pages on the same server.

ii) Distributed – Information made up of many pages distributed on different servers.

- It is easy to use and provides information to anyone interested.
- In other words, it is a set of standards for storing, formatting, retrieving and displaying information using a client-server architecture, GUI interface and a hyper text language that enable dynamic links to other documents.

Intranet

Definition

- Intranet is the Internet based computing network that are private and secure.
- It may consist of many interlinked local area networks and also use leased lines in the wide area network.
- The main purpose of an intranet is to share company information and computing resources among employees.

Role of Intranets in B2B Applications

- Intranet provides organizations a flexible way to organise information that can be shared with others in controlled and expandable way.

Reasons For Using Intranets

1. Employee productivity - Dynamic information and increased accuracy.
2. Cost saving - Online information distribution versus paper and reduced maintenance costs.
3. Knowledge management - Lets you customise information to meet user needs.
4. E-commerce - Allows customised content, presentation and transactions.
5. Customer management improvements - Integrating business process with customer relationship management and client specific information improves business cycles.

Advantages

1. Publishing ease - An Intranet is an excellent platform for publishing information internally. It is easily deployable, as the ubiquitous Web browser is available for virtually every operating system.

2. Cost - Most organizations have already established TCP/IP networks, and the incremental infrastructure cost of adding Web servers to the network is well within even departmental-level budgets.

3. Ease of use - Corporate users already have Web browsers and can instantly access the information on internal Web sites.

4. Low maintenance - With information residing in only one place - the Web server - it is relatively easy and affordable to add new information or to update existing information and make it instantly available.

Disadvantages

1. Collaborative applications for Intranet are not as powerful as those offered by traditional groupware - For instance, Intranet include no built-in data replication or directory services for remote users, while groupware packages such as Lotus Notes do.

2. Short-term risk - There are limited tools for linking an Intranet server to database or other back-end mainframe based applications. Programming standards for the Web, such as common gateway interface (CGI) and Java, are fairly new and just maturing.

3. Less back-end integration - With Intranets, firms have to set up and maintain separate applications such as E-mail and Web servers, instead of using one unified system as with groupware.

Extranet

• An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers normally to a subset of the information accessible from an organization's intranet.

Advantages

1. Extranet helps in improving company efficiency and output by automating procedures that were done manually in the past. Automation can also decrease the scope of mistake.
2. Work is done quickly as compared to past manual system.
3. Extranets can help in improving relationships with main or potential customers by giving them correct, precise and efficient information.

4. Information can be modified, updated and changed immediately on an extranet. All approved members thus have instant access to the most advanced information.

Disadvantages

1. Extranets can be costly to apply and maintain within an organization.
2. One of the big problem is the protection of extranets when dealing with precious information. System access should be controlled and checked properly to protect the system and information going into the incorrect hands.
3. Extranets can decrease personal face-to-face contact with clients and business partners. This can cause a lack of communication between employees, clients and organization.

Applications Of Extranet

Technology   Applications

1. Secure Electronic Mail -   B2B Communications
2. Bulletin Board -   Subject review and response vehicle, FAQ (Frequently   asked questions)
3. Instant Messaging -   Sales and customer support
4. Document Repository -   Knowledge management and customer support
5. FTP -   Customer support, sales support, software development

Difference between Intranet And Extranet
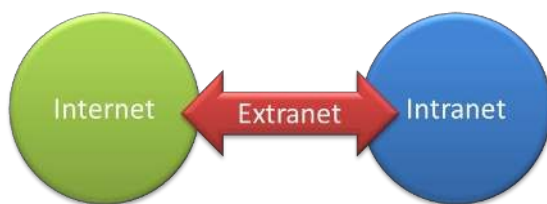
Intranet

• It facilitates sharing of information by people in single organization.
• Intranets are internet based computing networks that are private and secure, typically used by corporations, govt. for making resources more readily available to employees.
• It is an internet - like network within an organisation.

Extranet

• It facilitates sharing of information by individuals in multiple organisations.

- It provides wide area networks that run on public protocols with the goal of fostering collaboration and information sharing between organisation.
- It is a network that links selected resources of the intranet of a company with its customers, suppliers and other business partners, using the internet or private networks to link the organisation's intranets.

Virtual Private Network

- A VPN is a secure network that uses the internet as its main backbone network, but relies on the firewalls and other security features of its internet and intranet connections and those of participating organisations.
- Many organisation use VPN to establish secure intranets and extranets.
- VPNs would enable a company to use the internet to establish secure intranets between its distant branch offices and manufacturing plants and secure extranet between itself and its customers and suppliers.
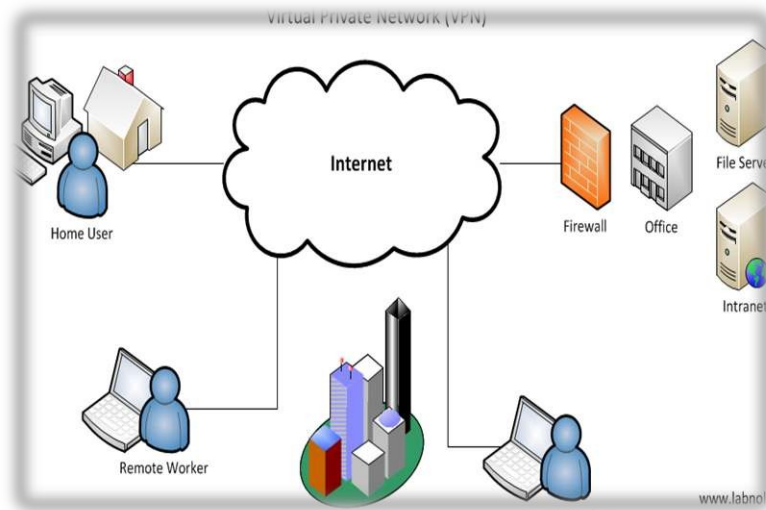
Building Own Website And Domain Registration

Reasons for building your own website

- A website of your own, with info about your family, or your business or even about your pet.
- It is the quickest way to let people all over the world know that you have arrived.
- Actors and actresses have their own websites with information about themselves and their movies. They only go to prove how vast the audience for this medium is.
- Any information that you would like to spread over a wide area economically could be done through your website – just put all the information in place, decide how you want the world to see it… and presto, you are on!

Benefits of the website

The benefits of having a website are many. It may be looked from a business-oriented point of view or from other forms of media promotions.

COST:

- Cost is a prime importance in any business. Setting up a website is one of the cheapest forms of promotion. Consider the alternatives: newspapers charge a sizable amount for limited space where you can say that you want to.
- Radio and television are good media, but their rates are likely to be out of your budgets.
- On the other hand, a website can be designed at a negligible cost, and yet give you ample space to showcase your company and your services.

TIME:

- Time is most essential factor from all others.
- Without using the time effectively, we can sure lose something very valuables.
- If we place an ad on newspaper, it will be only there for like 24 hours.
- In case of radio/TV it will be of few seconds or maybe minutes throughout whole day repeating the same ad 10-20 times. But it won't be so effective due to it is so less in time.
- Now comparing these with our own website, which is on Internet for a period of one whole year this sounds quite awesome.

REACH:

- Reach is another important factor for any sort of promotion.
- The publisher/advertiser is always concerned about the size of the audience he will cover by his promotion.
- One can never be sure if the message has been received-especially since people tend to go to the refrigerator for a snack or make that important phone call when the ads come in on TV.
- With newspaper ads there are simply too many of them on the same page.
- But you can have a full attention to your website since the person browsing your website is paying money to his/her ISP for their internet.

- Again he/she probably goes to your site because of some recommendations or he queried for it in a search engine.
- Last there is nothing on your website to distract him from your sales unlike the newspaper ads.

DOMAIN:

- A domain name is textual representation of a numeric number (IP address) used to locate specific areas of the internet. It is easier to remember a name rather than a series of numbers.

TYPES OF DOMAINS

There are 4 types of domains available for registration.

1. .com (it used to be a way for a web site to convey its publishing intent.)
2. .net (it is a top-level domain originally for network providers.)
3. .org (it is a top-level domain for non-profit organizations.)
4. .int (it is a domain meant for internet infrastructure providers, possibly large ISPs etc.)

The one site that uses this extension is The Phone Company(www.tpc.int) which provides free e-mail to fax services.

Domain Registration

- The procedure of registration of a domain name is not simple. First, we have to check if the desired domain name is available or not. There are some domain hoarders who registers good domain names just to blackmail future prospective customers, what we have to do is type our desired domain name in the form on www.internic.net which will tell you if it registered or not.
- Now to actually register there are two methods. The short-cut is a local Internet company do it for you and of-course the long one is do it yourself. Making a local internet company do the registration for you is quite awesome because you don't have to bother yourself having trips to bank, couriers etc. which will be a really headache.
- Now go to www.networksolutions.com and find tour way into the registration area. There is a field which will let you check if your domain name avails, if it is you can add it to your order.
- On the next step you will see your order listed along with few blank spaces left to fill up by you about your name, address, email etc.
- Every registered domain name has a total of four people involved in its maintainance.

Those are:

1. Registrant: who ultimately has authority over domain
2. Administrative contact: who is a decision maker in cases such as transfer of domain
3. Billing contact: the person who gets the bill
4. Technical contact: the person responsible for hosting the website.

Since you are registering a domain name independently, you can use the registrant's info as billing, Administrative and technical contact.

Now specify a name-server which will handle your domain.

Now you can submit the form and you will be taken to confirmation page. An agreement will be e-mailed to you which you have to reply to in order to complete the transaction.

Now you have to pay the money, just take the invoice to the bank which was sent by Network Solution and they will tell how to do it.

Your domain name will be registered as soon as you submit the application and you can have a 3-month grace period in which your payment must reach them.

Web Promotion

Web promotion

- Website promotion is the continuing process used by webmasters to increase exposure of a website to bring more visitors. Many techniques such as web content development, search engine optimization, search engine submission, and viral marketing are used to increase site's traffic.
- Approximately there are 30000 new websites that flood the internet daily in addition to 5 million sites already existing.
- Most companies stop after getting themselves a website and then after a few months down the line complain that their internet project didn't work and they now regret all those investments they made. This is the usual concern of those who does not know about the principles of world wide web and basics of selling products on the net.
- Once the web site is complete, it needs promotion.
- Without effective promotion any website would be lost in the maze of the Internet.

Target e-mail

- Target e-mail a very productive method of getting online results.
- It is also known as e-mail marketing.
- It is an email directly sent to a group of people.
- It normally involves ads, request business, sales or donations, and is meant to build loyalty, trust, or brand awareness.
- Hence it is very important that you do not use spamming as a marketing tool and rather only e-mail to certain people who have agreed to receive emails on topics related to your site.
- Such lists of addresses can be purchased from places like www.yesmail.com or other such sites.

Banner Exchange

- A banner exchange is a group of web sites that exchange advertising with each other. Each web site has a banner advertisement that displays other web sites' banners. By displaying ads on their web site, banner exchange members generate free Advertising and site-linking for their own banners.
- So, the more hits that you get, the more banner views you earn on other site and hence you further increase your hits. There is a general click-through rate of 2% which means 2 out of every 100 people who see your banner will visit your site.
- Example: A good banner exchange site is Microsoft's www.linkexchange.com

Shopping bots

- Shopping bots are like one of the search-engines.
- A shopping bot is an online price comparison software tool which automatically searches the products of many different online stores to locate the most affordable rates for customers.
- There are some well-known and popular bots.

Bottom Dollar.com(www.bottomdollar.com)

- Like other bots, bottomdollar.com lets you pick a category and search from there. The bot searches all the major merchants for each category and lets you sort results by price.
- Links to products often took up to merchants, home pages and not to the products themselves and the prices were sometimes inaccurate.

Excite Shopping(www.excite.com/shopping)

- Excite's product finder covers a limited number of categories. Unlike other bots, it doesn't look for book and music.
- For other categories like computer hardwares are broken down into useful sub-categories such as monitors,laptops,desktops.
- Here you can search for products as well as reviews.

My Simon(www.mysimon.com)

- It queried so many sites(over 1000). It did a better job of finding the best deals than the other shopping agents.
- It offers dozens of categories, which cover just about any item you are likely to buy on the web.
- you can also search for auction sites(E-bay) and classified ads.

Web market(www.webmarket.com)

- It covers specifications of products such as books , consumer electronics and office supplies but within these categories you are limited to specific types of good like modems , printers but not PDAs in consumer electronics.

Yahoo! Shopping(www.shopping.yahoo.com)

- This bot searches yahoo merchants(those vendors that sell through portal),initially. Only when this search has been completed, you can choose to search other merchants .
- when you enter key words, yahoo! Scans its database and lists all items that fit the description. You click on best match and the bot searches only that product , eliminating all irrelevant hits. Yahoo! also searches auctions but only its own.

UNIT - 3

Internet Security

The internet based communication security can be grouped under 3 categories:-

1. Authorisation,
2. Authentication and
3. Integrity

Authorisation

Client server network security problems occur in 3 ways

1. Physical security holes
2. Software security holes
3. Inconsistent usage holes

1.Physical security holes

Eg: In public workstation,where no precaution is taken,a hacker easily reboot the system and tamper with files.

Eg : on the network, hackers get access to the network system guessing passwords of various users,

2.Software security holes

(Badly written program or privileged software are doing things they shouldn't)

Eg:- rlogin hole in IBM RS-6000 workstation, enables the malicious crackers to create a 'root' sell or super user acess mode-a highest level of access possible, to delete the entire file system or to create new account or a password file resulting in a highest damage.

3.Inconsistent user holes

When a system adminstrator assembes a combination of hardware and software such that the system is seriously flawed from a security point of view.

A security hole is created by the incompatibility of attempting two unconnected but useful things. Problems like this are difficult to isolate once a system is set up and running.

Protection methods

* Access control –specifies the resources,various users and groups who entitled to access.

In e-commerce, several methods have been developed in recent years:-

- Trust based security

- Security through obscurity(quality of being hard to understand)

- Password schemes

- Biometric system

Authentication

A process to verify the identity of a user as they log onto a network.

Ex: If the request originates from unauthorised client , many servers are configured to reject a request. The server verifies the authorisation of the client to undertake the specific task before granting service.

In case of client:- If a client program is responsible for sending e-mail and the same contains sensitive information,the client may need to verify that it is communicating with an impostor.

Ex- IP address is one type authentication, the server examines the source IP address on each incoming request and only accepts the requests from client computers on the authorised list.

Trusted Services

- How can the client and server programs know that they are not communicating with impostors?
- It is therefore a trusted service to be provided.
- It uses a public key encryption system.

Trusted based security

- TBS is to trust everyone and do nothing extra for protection.
- Assume all users are believable and competent in their use of shared network.

Categories of Authentication

Authentication

1. User-to-host
2. Host-to-host
3. User-to-user

1.User-to-host

Host identifies users before providing services for which users are authorised and deny those services for which they are not authorised.

2.Host-to-host

Possible for an intruder to potentially masquerade as another computer system and gain access to a number of unprotected computer systems around the world. This is prevented by applying encryption algorithms

3.User-to-user

 *Establishes proof of one user's identity to another user.

* Employed as a form of digital signature with electronic mail.

Threats in Password

- common word or proper names
- Texas airforce base by n/w adminstrator-They could crack about 70 % of the passwords on their unix networks

- Dictionary comparision

- Password in remote log-in session

To come out of above threats ,it is suggested to have various approaches for creating one time passwords, including:

1. Smart cards
2. Randomised token
3. Challenge response schemes

Password Do's

1. Use a password generator run to

generate one time only password.

2. Password with atleast 8 character long

With one non alpha-numeric character.

Password Don'ts

1. Do not use words,or variation of

      Words,pairing of short words.

2. Do not use only number digits like

12345 or repeated character strings AAAABBB.

Do not use Symbols or words from a foreign language.

3. Passwords to change if used continuously once in 60 to 90 days on Regular basis or even earlier.

3. Do not use a portion or variation of your real name,office or home Address or phone number etc.

4. Run a password guesser to test the security of your own system's password.

Integrity

Integrity refers to the condition of data after it has been transmitted to another location as compared to its original condition. It is possible that as a file, electronic mail or data is transmitted from one location to another, its integrity

May be compromised due to interruptions or interference in communication lines or human intervention.

Transaction security

An online transaction requires a consumer to disclose sensitive information to the vendor in order to make a purchase, placing himself at significant risk. Transaction security is concerned with providing privacy in transactions to the buyers and sellers and protecting the client-server network from breakdowns.

- Client security- Techniqes and practices that protect user privacy and integity of the computing system.

- Server security- Protect web server, software and associated hardware from break-ins, vandalism and DOS attacks.

- Secure transactions- Guarantee protection against eavesdropping and intentional message modification(tapping,intercepting,diverting)

Security Issues in E commerce

1.Malicious code:- It includes a variety of threats such as virus, worms , Torjan horse etc.

- Virus- A virus is a computer programme that triggered by the activation of their host and spread to other files, deliver a pay load include macro virus, script virus, file infecting virus.
- Worms –It is a stand-alone malicious programs that can self replicate and propagated independentlyas soon as they have breached the system.

2. Unwanted programmes:-There are programmes installed without the user consent.

- Browser Parasites- Programmes used to monitor and change settings of a user's browser.
- *Adware- Unwanted pop up ads
- Spyware- Programmes used to obtain personal information

3. Phishing and Identity theft- It refers to any deceptive , online attempt by third party to obtain confidential information for financial again.

4. Hacking

- Hacker- An individual who intends to gain unauthorised access to computer systems.
- Cracker-A hacker with a criminal intent.
- Cyber Vandalisim-Intentionally,disrupting, defacing or destroying a web site.

5. Credit Card Fraud- It refers to use of stolen data to establish credit under false identity.

6. Spoofing- hackers hide their identity, misrepresent themselves by using fake email

Addresses or masquerading as someone else this threatens integrity and authenticity of the hacked website.

7. DOS (Denial of Service)- Hackers flood a website with useless traffic to inundate or overwhelm the network.

8. DDOS (distributed DOS)- Hackers are numerous networks from numerous launch points to send useless traffic to a website.

9. Sniffing-A sniffer is a type of eavesdropping application that monitors information travelling over the network. It enables hackers to steal proprietary information from anywhere on a network including email, files, reports etc.

10. Insider jobs- It involves poorly designed server and client software and complexity of programmes which increase vulnerabilities for hackers to exploit.

Defensive measures against Security Issues in E commerce

1. Encryption

2. Secure socket layer- The SSL protocol provides data encryption, server authentication,client authentication and message integity for TCP/IP connections. It prevents eavesdropping, tampering or forgery when data is transported over the internet between two applications.

3. Secure hypertext transfer protocol- It is a secure oriented communication protocol designed for use in conjunction with HTTP enabled secure connection and individual message transmission. Under SHTP a message may be signed, authenticated or encrypted.

4. Trust Seal Programmes- Trust seals have been developed to provide assurance about web businesses practices and policies.

5.Digital Signature-It is a signature in encrypted electronic code which is encrypted by the sender with his private key and can be decrypted only with the public key of the SENDER(by receiver)

6. Digital Certificate- It is a digital document issued by a trusted third party institution known as certificate authority that certifies the name and identifying information of the company. It is signed with the private key of the certificte authority. Therefore,its authenticity can be known by knowing the public key.

A digital certificate contains

- The name of the company
- Public key of the company
- Digital certificate serial number
- Expiry date/date of issue
- Digital Signature of the certificate Authority

Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet.

How SET works:

Assume that a customer has a SET-enabled browser such as Netscape or Microsoft's Internet Explorer and that the transaction provider (bank, store, etc.) has a SET-enabled server.

1-The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.

2-The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.

3-Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.

4-The customer places an order over a Web page, by phone, or some other means.

5-The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.

6-The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.

7-The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.

8-The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.

9-The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.

10-The bank digitally signs and sends authorization to the merchant, who can then fill the order.

Computer monitoring

Monitoring software records and logs all incoming/outgoing network traffic, user processes and interactions and application activities.

Adv

1-Identifying errors during the process

2-Identifying the strength of the work force

3-ensuring safety

4-Adherence(agreement) to policy- disobey the policies.

Disadv

1-Expensive Process

2-Create trust issues

3- Stressful atmosphere

4- Kills creativity

Internet Privacy

It is the privacy and security level of personal data published via internet.

Internet privacy risks include

1.phishing- An internet hacking activity used to steal secure user data, including user name,password,bank account number,security pin or credit card number.

2.*Pharming- An internet hacking activity used to redirect a legitimate website visitors to a different Ip address.

3.*spyware- An offline application that obtains data without a user's consent. When the computer is online,previously acquired data is sent to the spyware source.

4.Malware- An application used to illegally damage online and offline computer users through Torjans,viruses and spyware.

Internet privacy violation risks may be minimized as follows

Always use preventive software applications such as anti-virus,anti-malware,anti-spam and firewalls.

* Avoid shopping on unreliable websites

*Avoid exposing personal data on websites with lower security levels.

*Clear browser,s cache and browsing history on a consistent basis.

*Always use very strong passwords.

Email privacy

Email privacy is the broad topic dealing with issues of unauthorized access and inspection of electronic mail. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers or on a user computer.

Email has to go through potentially untrustworthy intermediate computers (email servers, ISPs) before reaching its destination, and there is no way to verify if it was accessed by an unauthorized entity.

Technological workarounds

1.Encryption

2.Transport level encryption

 It is a TLS (SSL) layer over the plaintext communication, allowing email servers to upgrade their plaintext communication to encrypted communication. Assuming that the email servers on both the sender and the recipient side support encrypted communication, an eavesdropper snooping on the communication between the mail servers cannot see the email contents. Similar extensions exist for the communication between an email client and the email server.

3.End to end encryption

In end-to-end encryption, the data is encrypted and decrypted only at the end points. In other words, an email sent with end-to-end encryption would be encrypted at the source, unreadable to service providers like Gmail in transit, and then decrypted at its endpoint. Crucially, the email would only be decrypted for the end user on their computer and would remain in encrypted, unreadable form to an email service like Gmail, which wouldn't have the keys available to decrypt it.

CYBER CRIME AND ITS PREVENTIONS

Introduction

Computer Crime is the use of computer resources to engage in unauthorised or illegal acts.

It is caused by criminal or irresponsible actions of the computer users who are taking advantage of widespread use of computer networks in our society.

DEFINITION

According to the Association of Information Technology Professionals(AITP),the definition of computer crime includes the following :

- Unauthorised use , access ,modification and destruction of hardware , software, data or destruction of network resources.
- Unauthorised release of information.
- Unauthorised copying of software.

TYPES/FORMS OF CYBER CRIME TODAY

Money Theft:

- It involves fraudulent alteration of databases and accounts of various employees of an organization leading to immediate transfer of funds to the account of criminals.
- This results in financial loss to the organisation as well as the customers
- Example : Theft of 11million from Citi Bank in 1994.

Service Theft:

- It is the unauthorized use of computer systems and network in an organization .
- Example : playing games through internet in the pc of the organisation, doing personal and private transaction through internet connection of the organization/ company.

Software Theft:

- Computer Programs are valuable property   and   thus are the subject of theft from computer system in an unauthorized manner . Unauthorized copying is illegal because software is an intellectual property that is protected by copyright law and user licensing agreements.
- Example : software piracy, lotus development corporation developed software whose copies were marketed and new clones were made.

Data Altertion or Theft:

- Making illegal changes or stealing data is another form of computer crime. For e.g. changing grades of students in an institution by taking bribes may affect their career   and   life. Changing the credit card information and data in the id proofs results in innocent persons being attacked by criminals.

Malicious access

- One of the obsessive use of computers in an unauthorised manner is computer hacking. Hackers commit electronic breaking and entering i.e. they access to a computer system read important files but may or may not steal anything. This results in leakage of high priority information resulting in other criminal activities.

Computer viruses and worms

- One of the most destructive examples of computer crimes is the creation and spreading of computer viruses and worms.
- Virus is the program code when inserted through supportive programs copies its destructive routines into system and user programs . As a result data is destroyed .
- A worm is a program that runs by itself and destroys the memory contents and hard disk data.
- Viruses enter systems through illegal or burrowed copies of software or through networks links to other computer systems

Software package privacy

Anti-Virus Programs

1.Hardware Firewall System-Hardware-based firewalls protect all networked computers and are usually found in a broadband router. These firewalls use static packet filtering to analyze, pass, or stop incoming and outgoing packets based on IP address or source. It can block threats and add another layer of protection and privacy.

2.Cloud Data Storage System-A secure Cloud data storage system can also protect your business data and reduce the risk of theft if someone was to hack the main server.

3.Wi-Fi Encryption- It is an encrypted network only employees with a passcode can access. Prevent unauthorized access and intrusions by making sure the router is also password protected.

4.Email Protection-email protection program that can filter incoming messages, filter out and delete spam automatically, and also encrypt business-to-business communications for enhanced security. This adds another layer of protection for business communications and can prevent malicious software downloads and viruses that come through an email message or attachment.

5.Card Processing Fraud Prevention-Fraud management tools that can be integrated with existing systems. You could also invest in data encryption tools designed to protect cardholder data and reduce the costs of data theft.

6.Secured Network Access-Authentication and security tools can prevent unauthorized access to confidential business information, files, and documents stored on the company Intranet. Investing in the right set of data privacy tools for your business can reduce the risk of a data breach, theft, and malicious server attacks.

Prevention Techniques

1. Encrypt data and programs.
2. Beware of malicious contents.
3. Monitor system transactions.
4. Be social-media Savvy
5. conduct frequent audits.
6. Restrict system use.
7. Educate people in security measures.
8. Protect sources with passwords and access cards and virus detection and eradication software's.
9. Install latest operating system updates
10. Protect your e-identity.

ENCRYPTION & DECRYPTION

Encryption

Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext).

The main purpose of Encryption is to secure sensitive or confidential data stored on computer or transmitted via internet

```
Key ──── Symmetric key
     └─── asymmetrickey
```
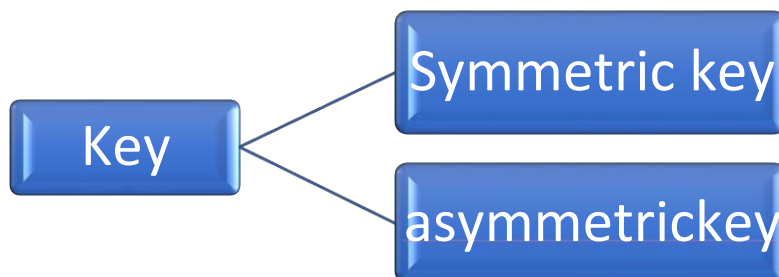
Private Key: This means that the encryption and decryption keys are the same. The two parties must have the same key before they can achieve secure communication.

Public Key: This means that the encryption key is published and available for anyone to use. Only the receiving party has access to the decryption key that enables them to read the message.

In an asymmetric cryptosystem (or public key cryptosystem), there are two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key.

Encryption

Secret key cryptography

Public key cryptography

## Hash functions
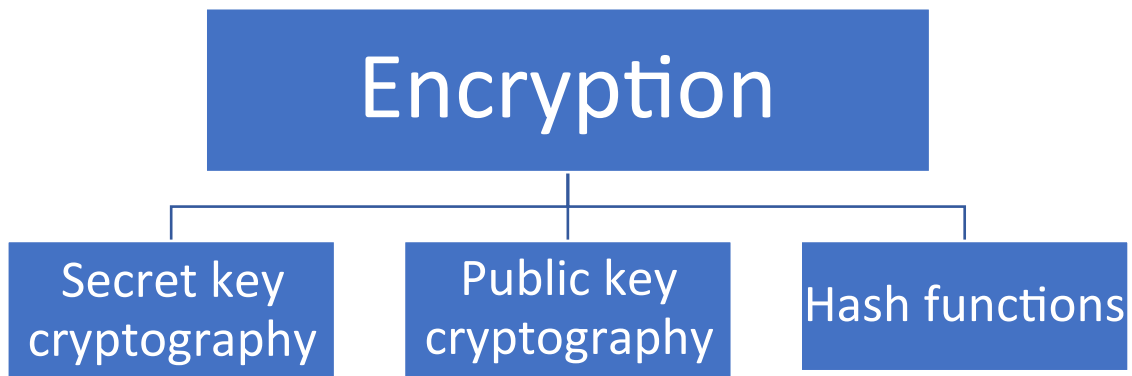
Secret key encryption
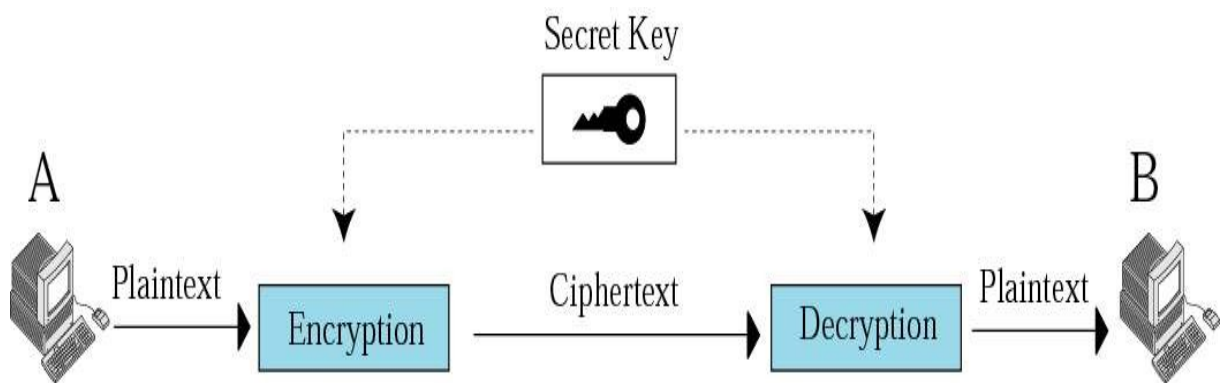
Advantages

- Very fast encryption and decryption of a message
- The bigger the code of the key, the greater the safety

Disadvantages

- Exchange of the key: It must be ensured that the key to encryption, will be exchanged via a secure channel (e.g. in person). However, in practice this can be really difficult
- The number of keys that are required: For each pair of participants that wish to exchange encrypted messages, a new key is required

Public key encryption
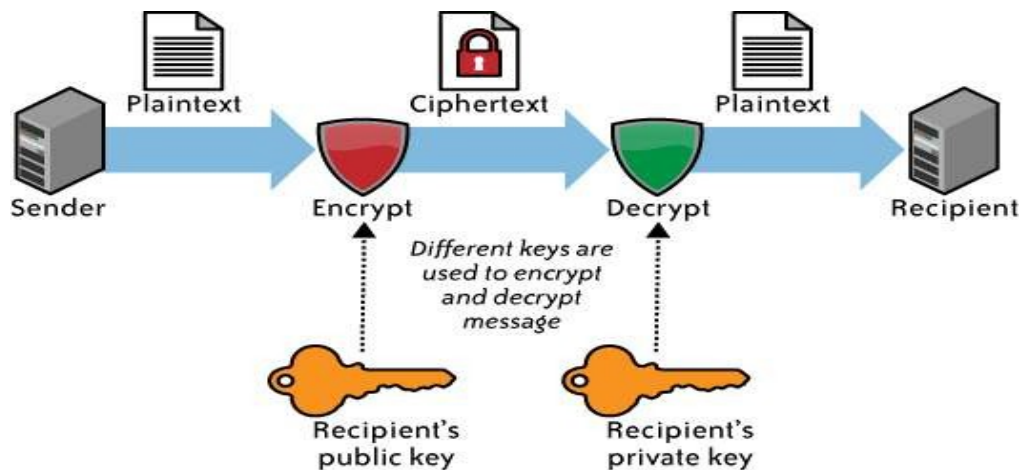
Advantages

• In asymmetric or public key cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.

• The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.

• Can provide digital signatures that can be repudiated

Disadvantages

• A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

Decryption

Decryption is the process of decoding encrypted information so that is can be accessed again by authorised user.

ENCRYPTION VERSUS DECRYPTION

ENCRYPTION
- Process of encoding a message or information in such a way that only authorized parties can access it
- Converts the original message to an unrecognizable message
- Occurs at the sender's end

DECRYPTION
- Process of transforming data that has been rendered unreadable through encryption back to its unencrypted form
- Converts the received encrypted message back to the original message
- Occurs at the receiver's end

Visit www.PEDIAA.com

Side-by-side comparison of symmetric encryption and asymmetric encryption

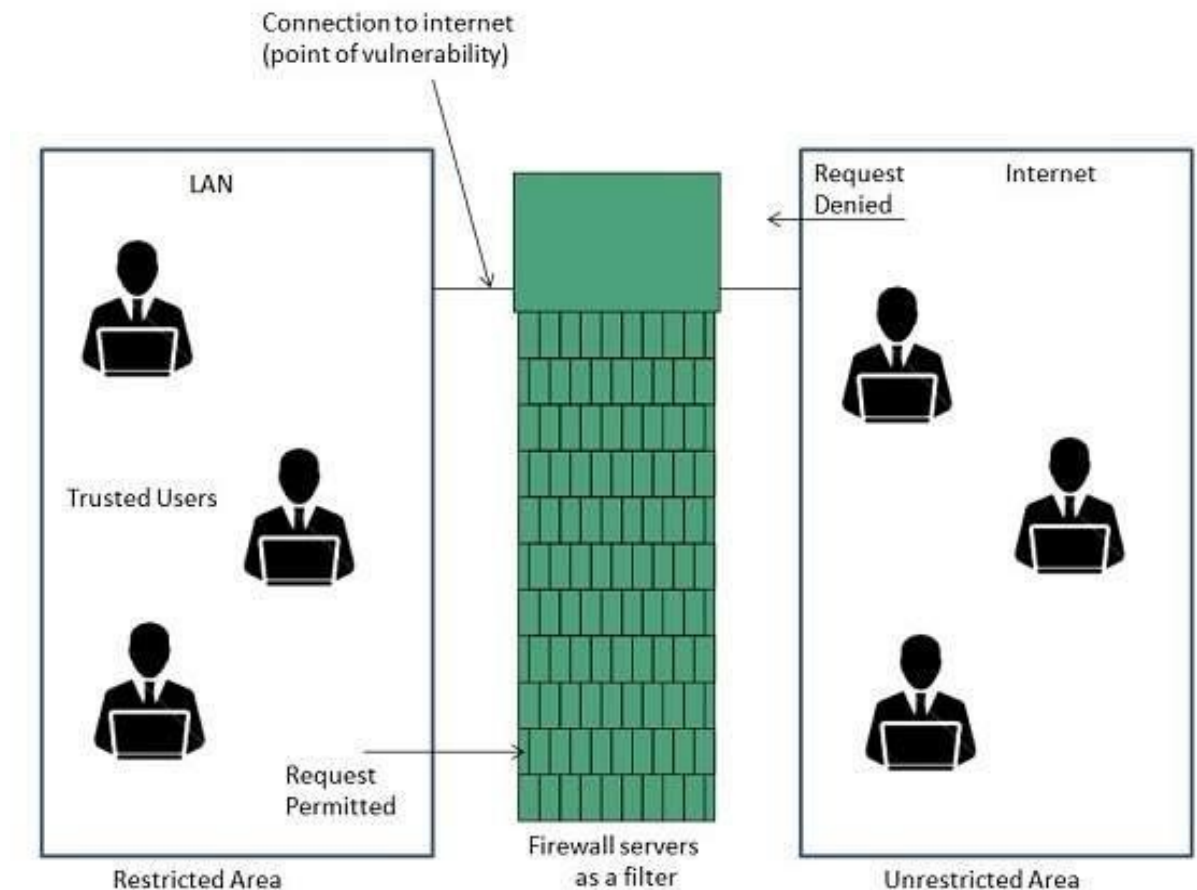| Comparison Factor	Symmetric Encryption	Asymmetric Encryption
Number of Cryptographic Keys	Symmetric encryption incorporates only one key for encryption as well as decryption.	Asymmetric Encryption consists of two cryptographic keys. These keys are regarded as **Public Key** and **Private Key**.
Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations.	Contribution from separate keys for encryption and decryption makes it a rather complex process.
Swiftness of Execution	Due to its simplistic nature, both the operations can be carried out pretty quickly.	Because of encryption and decryption by two separate keys and the process of comparing them make it a tad slow procedure.
Algorithms Employed	RC4 AES DES 3DES QUAD	RSA Diffie-Hellman ECC El Gamal DSA

Digital Signature

Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.
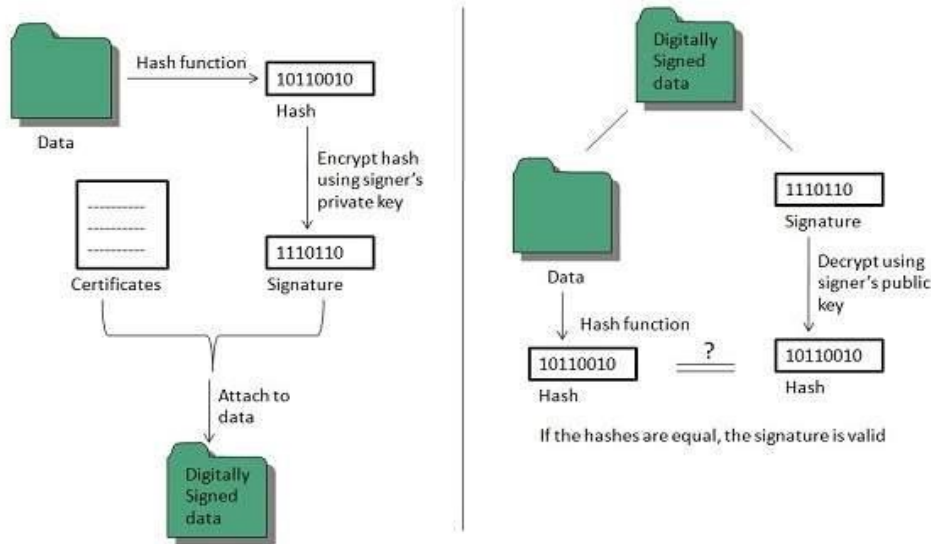
A digital signature should not only be tied to the signing user, but also to the message.

Firewall Security

- Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

- The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.

Connection to internet
(point of vulnerability)

LAN

Request Denied

Internet

Trusted Users

Request Permitted

Restricted Area

Firewall servers
as a filter

Unrestricted Area

There are two types of Firewall system:

One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

Types of firewalls

1. Packet filtering firewalls
2. Circuit-level gateways
3. Stateful inspection firewalls
4. Application-level gateways
5. Next-gen firewalls

Circuit-level gateways- These are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves,

Stateful inspection firewalls- State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This offers more security than either packet filtering or circuit monitoring alone

Application-level gateways- This kind of device, technically a proxy, and sometimes referred to as a proxy firewall, combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for

which they are intended -- as specified by the destination port -- but also by certain other characteristics, such as the HTTP request string.
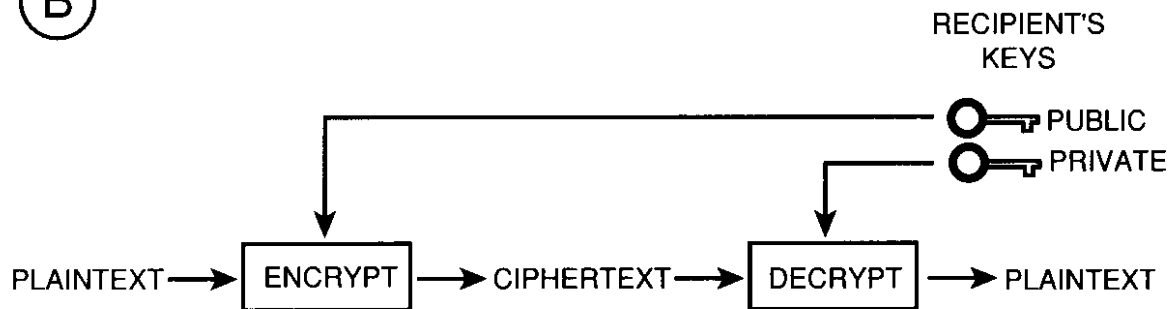
Next-gen firewalls - A typical next-gen product combines packet inspection with stateful inspection, but also includes some variety of deep packet inspection(deep packet inspection looks at the actual data that the packet is carrying).

Symmetric and Asymmetric Encryption Algorithms
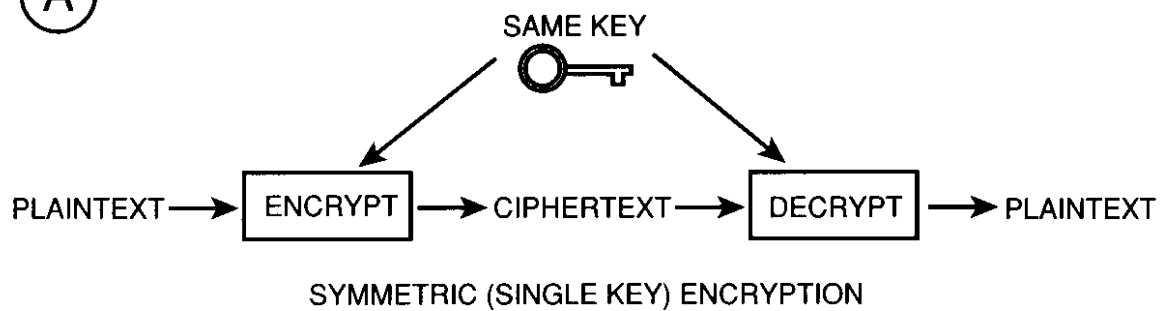
DES

Basics

- DES uses the two basic techniques of cryptography - confusion and diffusion.

- At the simplest level, diffusion is achieved through numerous permutations and confusions is achieved through the XOR operation.

DES - The 16 Rounds

- The basic process in enciphering a 64-bit data block and a 56-bit key using the DES consists of:

    - An initial permutation (IP)

    - 16 rounds of a complex key dependent calculation f

    - A final permutation, being the inverse of IP
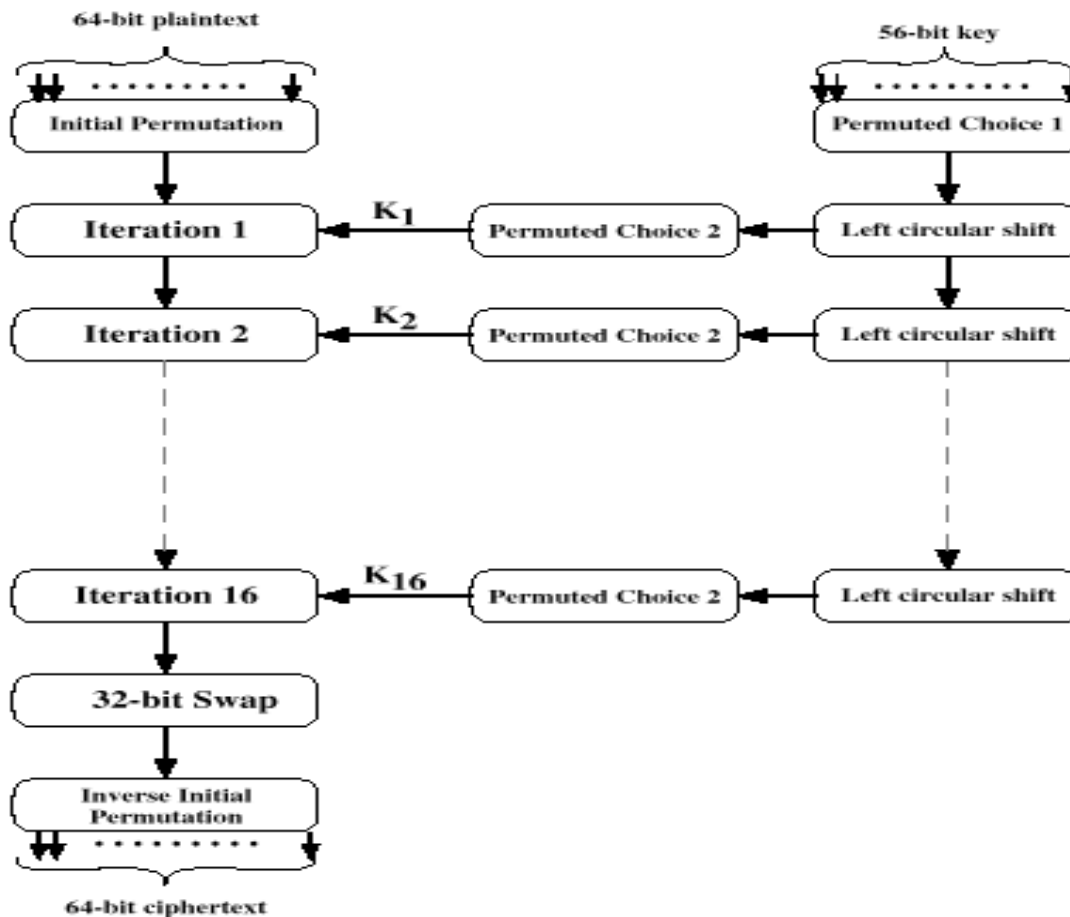
The Key Dependent Calculation
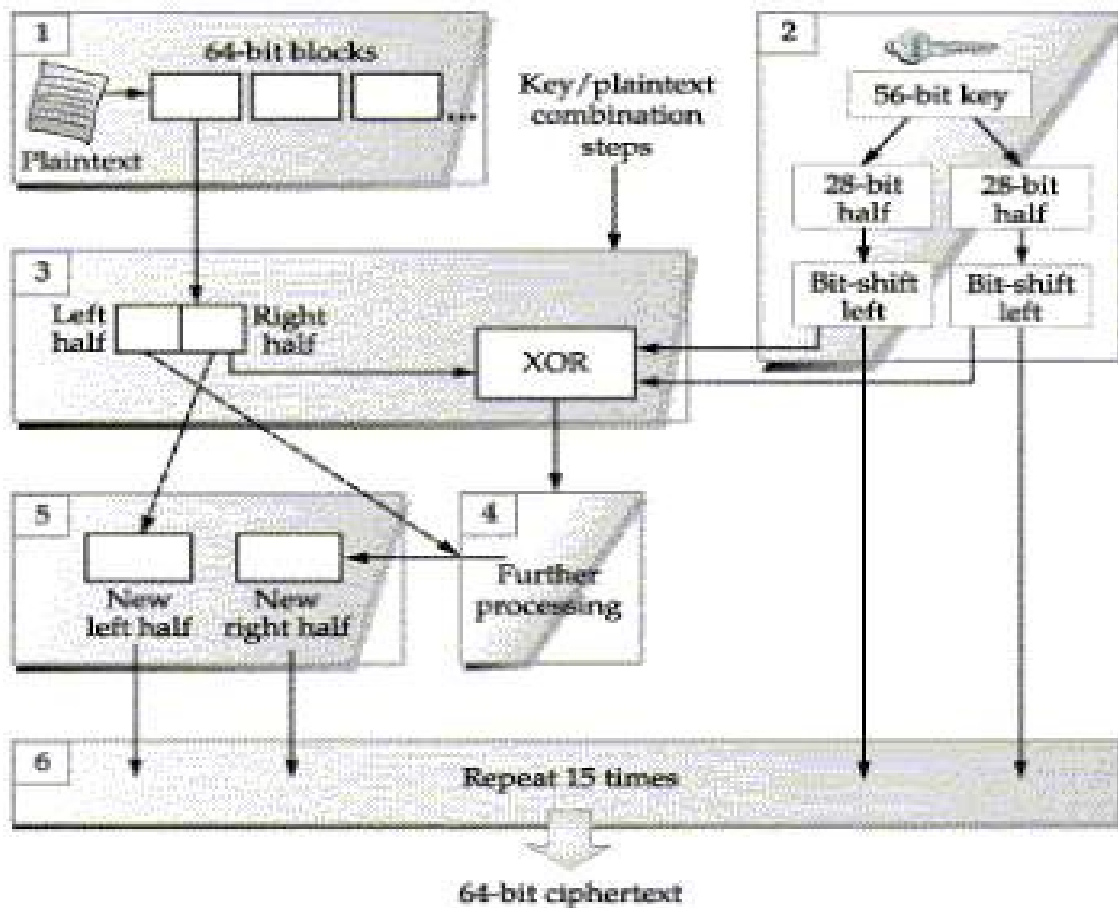
DES - Swapping of Left and Right Halves

- The 64-bit block being enciphered is broken into two halves.

- The right half goes through one DES round, and the result becomes the new left half.

- The old left half becomes the new right half, and will go through one round in the next round.

- This goes on for 16 rounds, but after the last round the left and right halves are not swapped, so that the result of the 16th round becomes the final right half, and the result of the 15th round (which became the left half of the 16th round) is the final left half.

RSA algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called *public key cryptography,* because one of them can be given to everyone. The other key must be kept private. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret.

RSA Algorithm

The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q

2. Calculate n=pq where n is the modulus for the public key and the private keys.

3. Calculate the totient: ø(n)=(p-1)(q-1)

4. Choose an integer such that 1< e <ø(n) ,and e is coprime to ø(n) ie: e and ø(n) share no factors other than 1; gcd(e, ø(n)) = 1.

 where e is released as the public key exponent.

5. Compute de to satisfy the congruence relation de   1 (mod ø(n)) ie:de=1+k ø(n)   for some integer k .where de is kept as the private key exponent.

Encrypting messages

Alice gives her public key (n & e) to Bob and keeps her private key secret. Bob wants to send message M

 to Alice.First he turns M into a number smaller than   n   by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c   corresponding to:

$$c = m^e \mod n$$

This can be done quickly using the method of exponentiation by squaring. Bob then sends   c to Alice.

Decrypting messages

Alice can recover   from   by using her private key   in the following procedure:

$$m = c^d \mod n$$

- Choose p = 3 and q = 11

- Compute n = p * q = 3 * 11 = 33

- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7

- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]

- Public key is (e, n) => (7, 33)

- Private key is (d, n) => (3, 33)

- The encryption of *m = 2* is *c = 2^7 % 33 = 2*

- The decryption of *c = 29* is *m = 29^3 % 33 = 2*

Firewalls

Firewall is device (usually a router or a computer) installed between the internal network of an organization and rest of the internet.

It uses two mechanisms:

a) Permits traffic

b) Block traffics

Permit Traffic:- A firewall may filter all incoming packets destination   and allow those packets which have permission.

Block   Traffic :- A firewall may filter all incoming packets destination   and block those packets which have no permission.

Types of Firewalls

A firewall is usually classified as :

1) Packet filter Firewall

2) Proxy based Firewall

Packet Filter Firewall :

- It can forward or block packets based on the information in the network layer and transport layer headers .

- It is a router that uses a filtering table to decide which packets must be discarded.

Example of filtering table

Packet filter firewall

To and from global internet ――― 1 ――― [ ] ――― 2 ――― Internal network

Interface	Source IP	Source port	Destination IP	Destination Port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Packets are filtered

1. Incoming packets from network 131.34.0.0 are blocked(security precaution).

2. Incoming packets destined for any internal TELNET server(port 23) are blocked.

3. Incoming packets destined for internal host 194.78.20.8 are blocked. The organisation wants this host for internal use only.

4. Outgoing packets destined for an HTTP server (port 80) are blocked . The organization does not want employees to browse the Internet.

Advantages and disadvantages

Advantages of firewalls:

1. Cheaper
2. Ideal for personal or home use
3. Easy to configure or reconfigure

Disadvantages of firewalls:

1. Sometimes difficult to remove or un-install a firewall completely.
2. Not suitable where response times are critical.

Proxy Firewall

Sometimes we need to filter a message based on the information available in the message itself(at the application layer).

Example :

Assume that an organization wants to implement the polices regarding its web pages: Only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port

80(HTTP).The solution is to install a proxy computer (application gateway), which stands between the customer(user client) computer and the corporation computer.
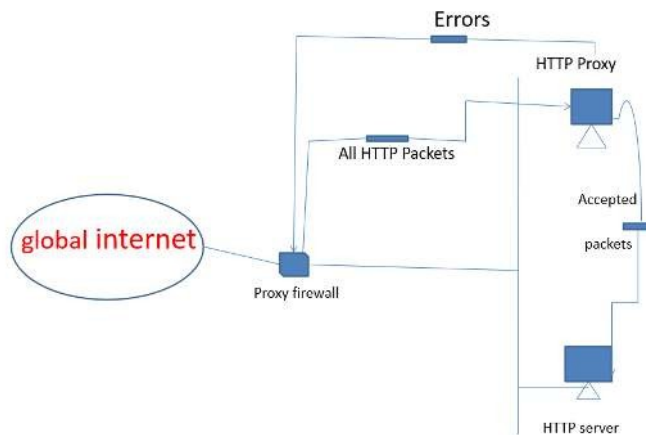
1. When the user client process sends a message, the proxy firewall runs a server process to receive the request.
2. The server opens the packet at the application level and find out if the request is legitimate.
3. If it is, the server acts as a client process and sends the message to the real server in the corporation.
4. If it is not, the message is dropped and an error message is sent to the external user. In this way , the requests of the external users are filtered based on the contents at the application layer.

Digital Signature

CONTENTS

- Introduction
- Motivation
- How does it work?
- Application
- Advantages
- Disadvantages
- Conclusion
- Reference

2

INTRODUCTION

- A digital signature is a mathematical scheme that is used to authenticate the sender of an electronic document .

- A digital signature is nothing but an attachment to any piece of electronic information, which represents the content of the document and the identity of the owner of that document uniquely

3

Motivation

- To provide Authenticity, Integrity and Non-repudiation to electronic documents.

- To use the Internet as the safe and secure medium for e-Commerce and e-Governance

4

Basic requirements

- **Private Key**

  The private key is one which is accessible only to the signer. It is used to generate the digital signature which is then attached to the message.

- **Public Key**

  The public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message

5

Digital certificate

- A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber.[1]

- But in case of any dispute between the two sides, there must be some entity with the receiver which will allow the receiver of the message to prove that the message was sent by the subscriber of the key pair. This can be done with the Digital Signature Certificate.[1]

6

Digital signature algo
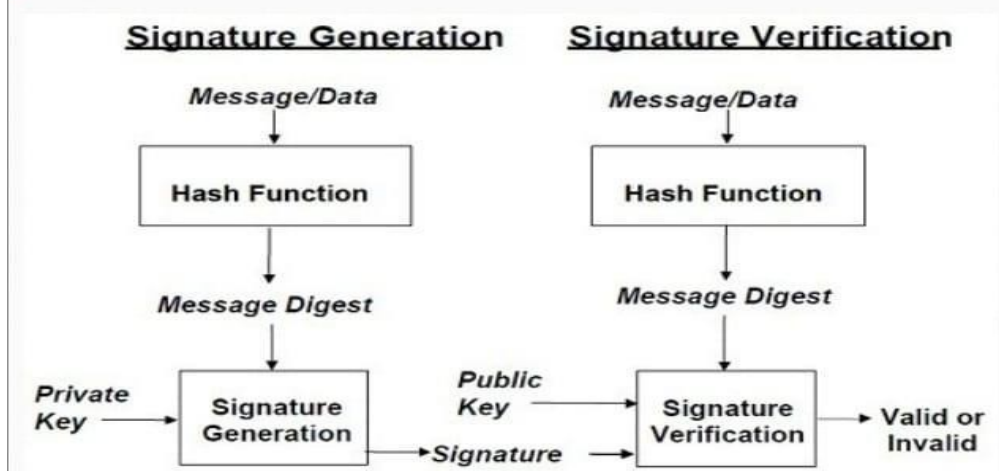
How does it work?
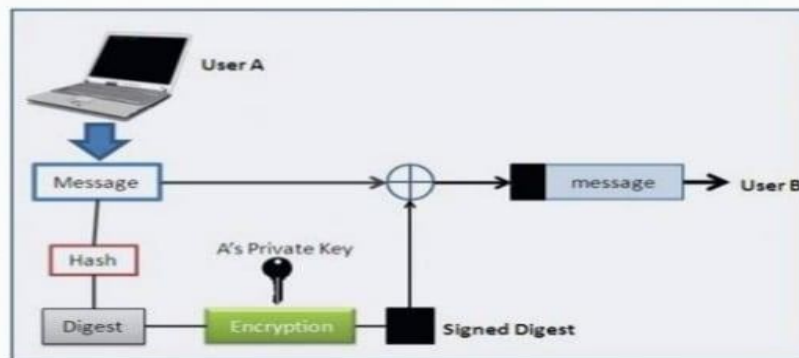
Application

➢ Electronic Mail
➢ Data storage
➢ Electronic funds transfer
➢ Software Distribution
➢ Smart Cards
➢ ISDN
➢ Time Stamped Signature
➢ Blind Signatures

9

Advantages

Authentication: Identification of the person that signs.

Integrity of data: Every change will be detected.

Non repudiation: Because the author cannot be denied of his work (he created and sent).

Imposter prevention: Elimination of possibility of committing fraud by an imposter

Disadvantages

Expiry: In this era of fast technological advancements, many of these tech products have a short shelf life.

Certificates: In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates.

Software: To work with digital certificates, senders and recipients have to buy verification software at a cost.

What are Digital Certificates?

A digital certificate (DC) is a digital file that certifies the identity of an individual or institution, or even a router seeking access to computer- based information. It is issued by a Certification Authority (CA), and serves the same purpose as a driver's license or a passport.

What are Certification Authorities?

Certification Authorities are the digital world's equivalent to passport offices. They issue digital certificates and validate holders' identity and authority.

They embed an individual or institution's public key along with other identifying information into each digital certificate and then cryptographically sign it as a tamper-proof seal verifying the integrity of the data within it, and validating its use.

What is the Process of obtaining a certificate?

1. Subscriber (sender) generates a public\private key pair. Applies to CA for digital certificate with the public key.

2. CA verifies subscriber's identity and issues digital certificate containing the public key.

3. CA publishes certificate to public, on-line repository.

4. Subscriber signs message with private key and sends message to second party.

5. Receiving party verifies digital signature with sender's public key and requests verification of sender's digital certificate from CA's public repository.

6. Repository reports status of subscriber's certificate.

What is the Process in obtaining a certificate?

Types of Digital Certificates

➤ There are four main types of digital certificates :-
- Server Certificates
- Personal Certificates
- Organization Certificates
- Developer Certificates

Server Certificates

➢ Allows visitors to exchange personal information such as credit card numbers, free from the threat of interception or tampering.

➢ Server Certificates are a must for building and designing e-commerce sites as confidential information is shared between clients, customers and vendors.

Personal Certificates

➢ Personal Certificates allow one to authenticate a visitor's identity and restrict access to specified content to particular visitors.

➢ Personal Certificates are perfect for business to business communications such as offering suppliers and partners controlled access to special web sites for updating product availability, shipping dates and inventory management.

Organization & Developer Certificates

➢ Organization Certificates are used by corporate entities to identify employees for secure e-mail and web-based transaction.

➢ Developer Certificates prove authorship and retain integrity of distributed software programs e.g. installing a software on a computer system in most instances requires what is called a "serial key"

What Does a Digital Certificate Contain?

It contains your name, a serial number, expiration date, 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 so that a recipient can verify that the certificate is real. Some digital certificates conform to the X.509 standard.

Why are they Used?

There are four(4) main uses:

1. Proving the Identity of the sender of a transaction

2. Non Repudiation – the owner of the certificate cannot deny partaking in the transaction

3. Encryption and checking the integrity of data - provide the receiver with the means to encode a reply.

4. Single Sign-On - It can be used to validate a user and log them into various computer systems without having to use a different password for each system

How do You Obtain An Individual's Public Key?

- When Alice wants Bob's public key:
  - Alice gets Bob's certificate (from Bob or elsewhere).
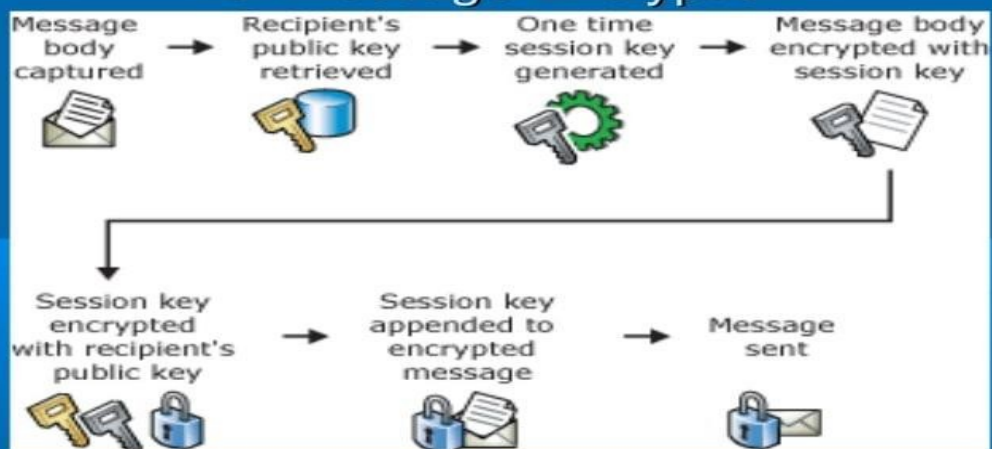 - apply CA's public key to Bob's certificate, get Bob's public key

K_B^+ → digital signature (decrypt) → Bob's public key K_B^+

CA public key K_{CA}

Where are Digital Certificates Used?

➢ **In a number of Internet applications that include:**

➢ 1.Secure Socket Layer (SSL) developed by Netscape Communications Corporation

➢ 2. Secure Multipurpose Internet Mail Extensions (S/MIME) Standard for securing email and electronic data interchange (EDI).

Where are Digital Certificates Used?

➢ 3. Secure Electronic Transactions (SET) protocol for securing electronic payments

➢ 4. Internet Protocol Secure Standard (IPSec) for authenticating networking devices

How Digital Certificates are Used for Message Encryption

Message body captured → Recipient's public key retrieved → One time session key generated → Message body encrypted with session key

Session key encrypted with recipient's public key → Session key appended to encrypted message → Message sent

Why do I need a Digital Certificate?

➤ Virtual malls, electronic banking and other electronic services are a commonplace offering service from the luxury of one's home. One's concern about privacy and security may prevent you from taking advantage of the luxury; this is where digital certificate comes in.

Why do I need a Digital Certificate?

➤ Encryption alone is not enough as it provides no proof of the identity of the sender of the encrypted information. Used in conjunction with Encryption, Digital Certificates provides a more complete security solution, assuring the identity of all the parties involved in a transaction.

UNIT - 4

ELECTRONIC DATA INTERCHANGE (EDI)

Contents

Introduction of EDI

• Electronic Data Interchange (EDI) is a set of standards for structuring information that is to be electronically exchanged between & within businesses, organizations, government entities & other groups, without human involvement.

• The main purpose of EDI is to save money and time because transactions can be transmitted from one information system to another through a telecommunication network , eliminating the printing and handling of papers at one end and the inputting of data at the other.

Working of EDI

1. Purchaser :

Department orders for an item to the purchasing department. Purchasing department prepares the purchase order and sends it to the vendor via its mail office under copies to accounts and shipping departments. Computer are involved everywhere but they are used for their own limited purpose.

2. Vendor :

Vender receives the P.O. from its mail office, route it to its sales. Sale department will take action through shipping and deliver goods to the receiving department of the purchaser. The copies of order confirmation, bill will be delivered to the mail office of the purchases.

EDI Example

Electronic Data Interchange (EDI)
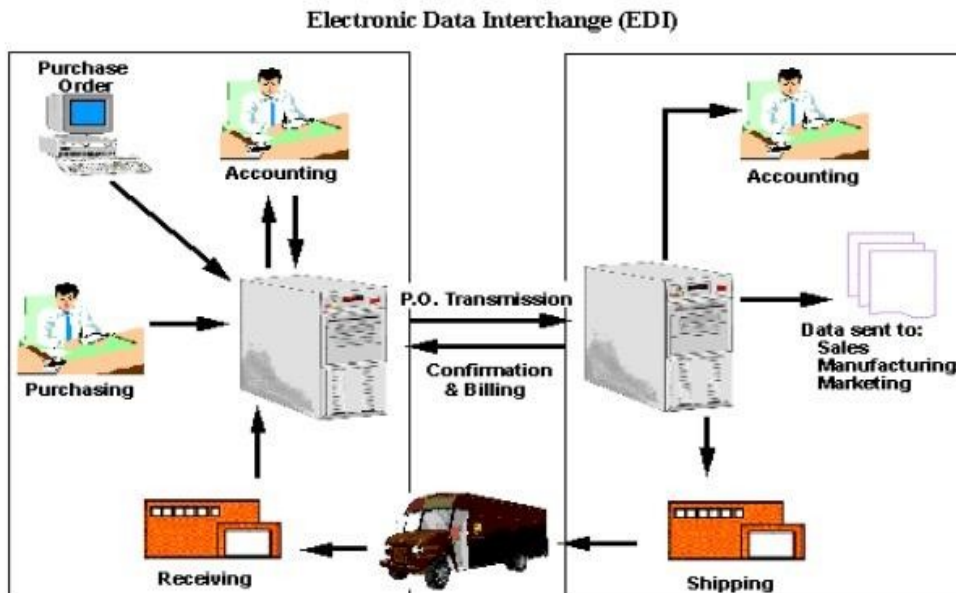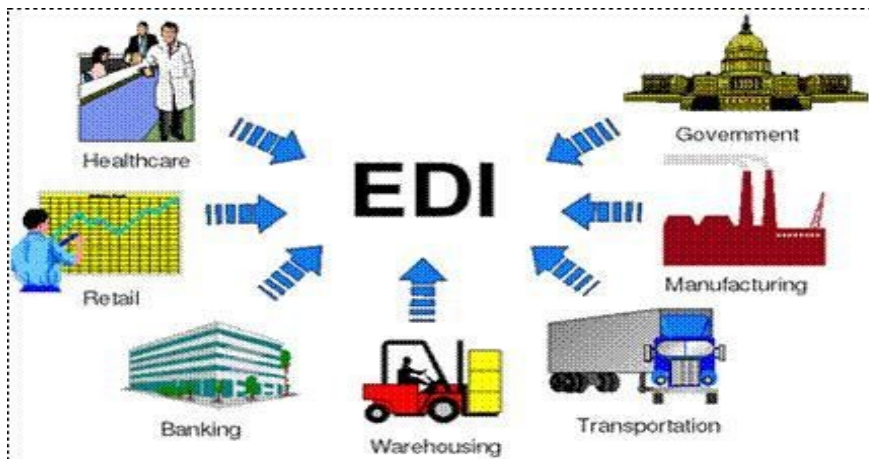

Key Requirements

To make EDI work properly, four key requirements exists.

These are :

1. Transaction standardisation
2. Transaction software
3. Appropriate mail box facilities
4. Legal restrictions

Applications of EDI

EDI is used in manufacturing, shipping, warehousing, utilities, construction, banking, retailing, government, healthcare and others.

Advantages of EDI

1. Quick access to information

2. Better customer service

3. Reduce paper work

4. Better communication

5. Increased productivity

6. Cost efficiency

7. Accurate and improved billing

8. Faster order placement

9. Reduction in error

Limitations of EDI

1. Firms have to incur extra cost for hiring and training staff.

2. Needs highly structured protocols.

3. Added security cost to safe guard confidential information from unauthorized access.

4. It does not allow consumers to communicate or transact with vendors in an easy way.

5. EDI application automate any certain portion of the transactions.

6. Application are narrow in scope.

Components of Electronic Data Interchange EDI

Standard Document Format – A standard format agreed upon by both parties which do not require complicated hardware or software to access information. Both parties communicate directly through a business application.

Translator and Mapper – A translator is used to convert the raw data into meaningful information according to specifications provided by a mapper. A mapper is used to create conversion specification. It compiles the specification and then gives instructions to the translator on how to convert the data.

Communication Software – A communication software is used to transmit data and convert business documents into a standard format. It follows a standard communication protocol which is incorporated in the software.

Communication Network – A communication network provides a direct link between trading partners who are will to exchange business documents through Electronic Data Interchange EDI.

- Modem – It is a hardware device that transmits data from one computer to another.
- VAN – A network that connect the computer system of one organization to another.
- Point to Point link – A direct communication link between two computers.

ELECTRONIC PAYMENT SYSTEM

Contents

Introduction

Electronic payment system are alternative cash or credit payment methods using various electronic technologies to pay for product and services in electronic commerce.

It means transfer of money before shipping of the ordered product. We have three ways to pay online: through cash, cheque, credit or debit card. Electronic fund transfer is an electronic transfer of information that equals moving funds from one financial institution to another.

Payment Types

It involves flow of funds inside corporations. These are of two types:

a) Payments received from customers

b) Payments made to suppliers

E-commerce helps in reducing these expenses by streamlining the cash collection and payment operations.

While automating the supply chain, the receipt and payment processing systems could be automated. The receipt of an actual product or confirmation of delivery to the customer could automatically be deposited.

Types of Electronic Payment System

Electronic Payment System is the transfer of money over the Internet .

TYPES:

1. Electronic funds transfer (EFT):

EFT is used for transferring money from one bank account directly to another . The money is deposited into account electronically. EFT is considered to be a safe, reliable, and convenient way to conduct business. EFT involves electronic transfer of money by financial institutions . Improved security is the main advantages of EFT.

2.PAYMENT CARDS:

A payment card is a plastic card containing information that can be used for payment purposes . It is used for:-

- ➢ getting cash from ATM
- ➢ pay online

3.Mobile payments:

Instead of using cash or cards a consumer can use a mobile phone to pay for a wide range of services and goods.

4.Online payment: This can be used for monthly payment for   Internet, phone bills, etc.

5. Peer to Peer:

A peer-to-peer payment service allows the transfer of digital cash (e-Cash) via e-mail between two people who have accounts at e-Cash-enabled banks. Peer-to-peer transactions allow online financial transfers between consumers. One example of peer-to-peer payment service is PayPal.

- ➢ PayPal is an online payment processor.
- ➢ Now owned by eBay.
- ➢ The first successful Internet-based e-commerce payment system.
- ➢ Trusted third-party between sellers and buyers.
- ➢ Securely stores credit cards data.

Categories of Electronic Payment System

1. Variations of digital cash, electronic money and coins.

2. Trusted third party.

3. Extension of the conventional notational fund transfer.

1.Variations of digital cash, electrical money & coins:

- • The thing actually being transferred is 'value' or 'money'.

- • Digital money, currency or coins are an encrypted serial number representing   money which are convertible to real money if desired.

- • It is a convenient form of existing money.

- Digital currency is very flexible since it can be made to behave like electronic cheques or anonymous cash.

2.Trusted Third Party:

- Maintains all sensitive information for its clients including buyers, sellers.
- Order information is transmitted along with information about payment confirmation and clearing.
- Does not include sensitive information.
- No real financial transaction is done online.

3.Extension of the conventional national fund Transfer:

- In credit card or cheque transactions, sensitive information is being exchanged.

- The information being transmitted online is encrypted for security.

- This system can be extended using internet which will provide more security.

- E.g.:- Cyber cash and VISA/Master card's SET-based transactions.

The Traditional Payment System

- This System uses currency,coins and cheques.Coins,currency can be used to mediate transactions by physical exchange.

- As cash payment have no audit trails many people ask for written receipts to show proof of purchase goods.

- Many people write cheques that tell the depository institution to transfer funds to the person/enterprise named on the cheque.

- The other system which are recently in use are :
    a)Value Exchange System

    b)Credit Card System

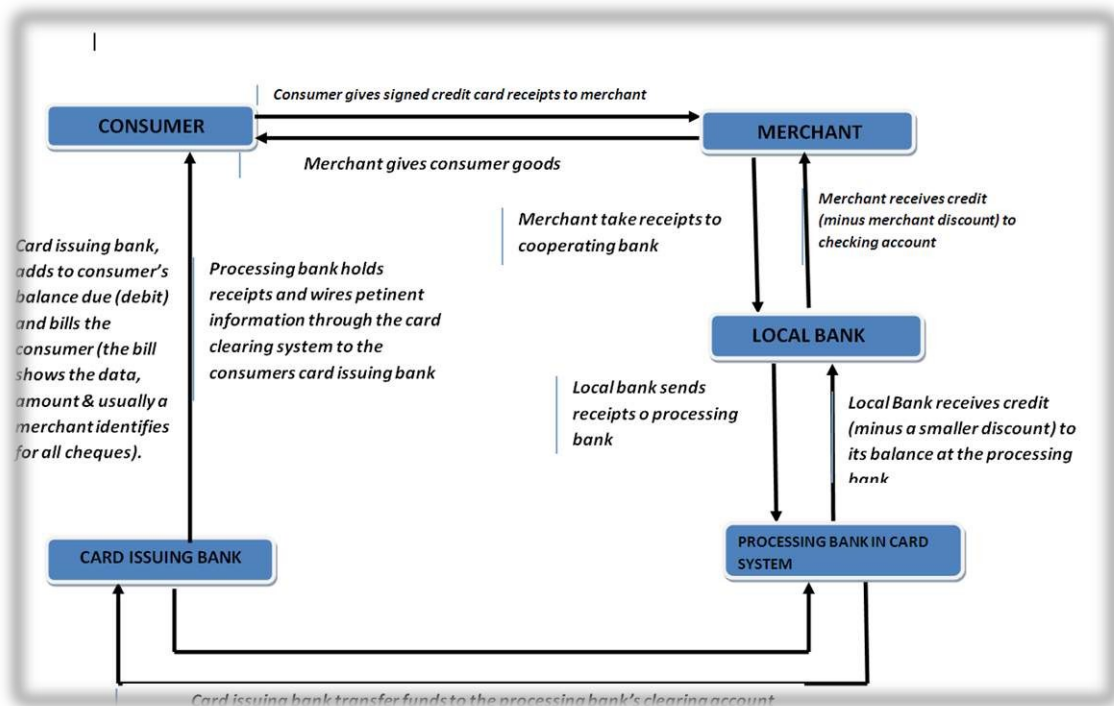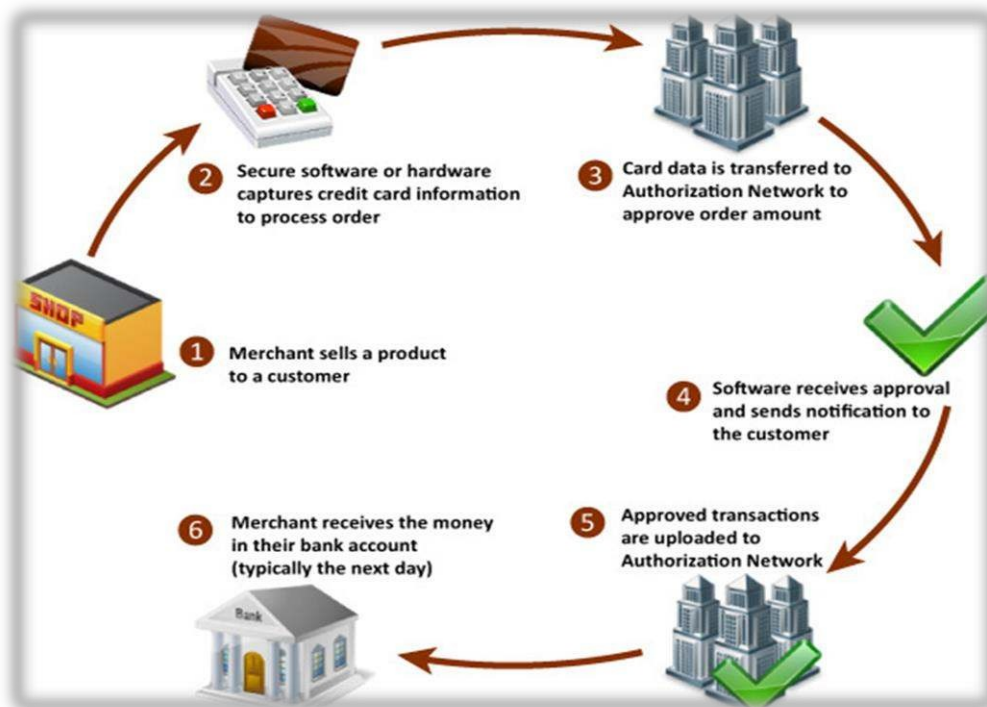   c)Electronic Fund transfer Systems

1. Value Exchange Systems:

- This can work much like cheque clearing system.

- The first widespread development of value exchange involved the use of credit cards.

- In such system , credit card holders' were exchanged for cash balances.

- Subsequently these have been used to transfer debits to both demand deposits and other accounts.

- The key element necessary for a value exchange is that of the value of the item exchanged can be readily determined and agreed upon.

- IOUs of credit card customers and margin account customers have a fixed monetary value.

2.Credit Card Systems

- Credit is money that a bank or credit card issuer lends you.

- You can get a loan for a specific purpose, such as financing a new car, buying a home. Using a credit card is like getting a loan.

- Every time you charge something, you're borrowing money until you pay it back later that month, or over time.

- In exchange for this loan, the credit card company adds interest charges to your account, which you must pay along with the purchase amounts.

- Here we will let to know that how credit card was used during traditional payment system.

3. Electronic Fund Transfer (EFT) Systems :-

- There are wide variety of electronic fund transfer (EFT) technologies. Many uses often require Automated Clearing Houses (ACHs). The most sophisticated EFT operations are connected to ACHs. ACHs can provide –

1. Credit transfers – Electronic credit transfer funds and information simultaneously from the payer to the payee. E.g., payroll, telephone bill payments.

Authorization to transfer funds
Funds transfer
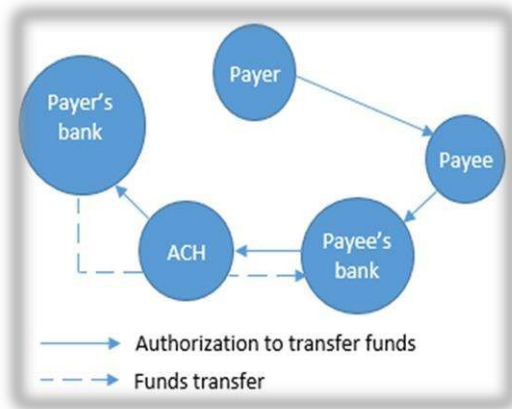
2. Debit transfers – Debit transfer funds from the payer's bank to the payee's bank, but only after the payer gives the payee valid authorization to do so. E.g., point of sale(POS).

Authorization to move funds
Movement of funds
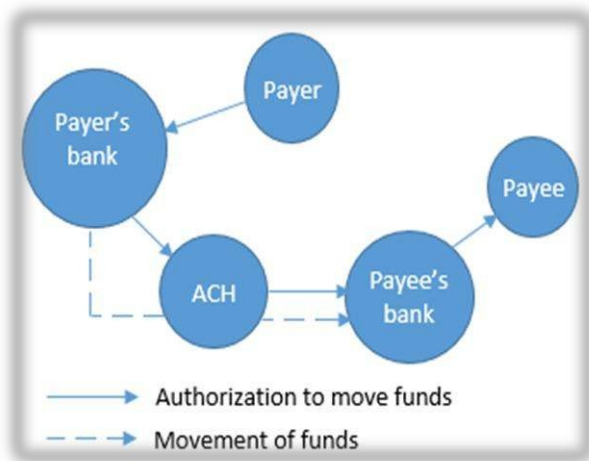
Automatic Deposits Of Payrolls And Social Security Payments :-

• As illustrated in electronic credit, the bank of the paying organisation gives ACH a computer tape that provides information of the banks and account numbers of the employees who are to be paid which in further the ACH uses to credit the amount to the receiver's bank.

Bill Payment By Telephone :-

This can be made efficiently through ACHs, using telephones or cable television lines. For this , depositors follows the steps mentioned as below:-

1.The depositor dials the bank.

2.Enter his account number, the amount he wishes to pay and the bank and account number of the recipient of the payment.

If the depositors provides data electronically, the payment information can be verified and entered directly on magnetic tape for submission to ACHs which will make the appropriate credit transfers.

GIRO(General Interbank Recurring Order)Funds Transfer Systems:-

- These are widely used in Europe.

- In this case, the depositor instructs a financial institution to make a payment to another individual who banks with another institution.

- The originating institution then transfers both funds and payment information telling which account should be credited to the receiving institution. Thus only one transfer is required for both funds and transmitted information.
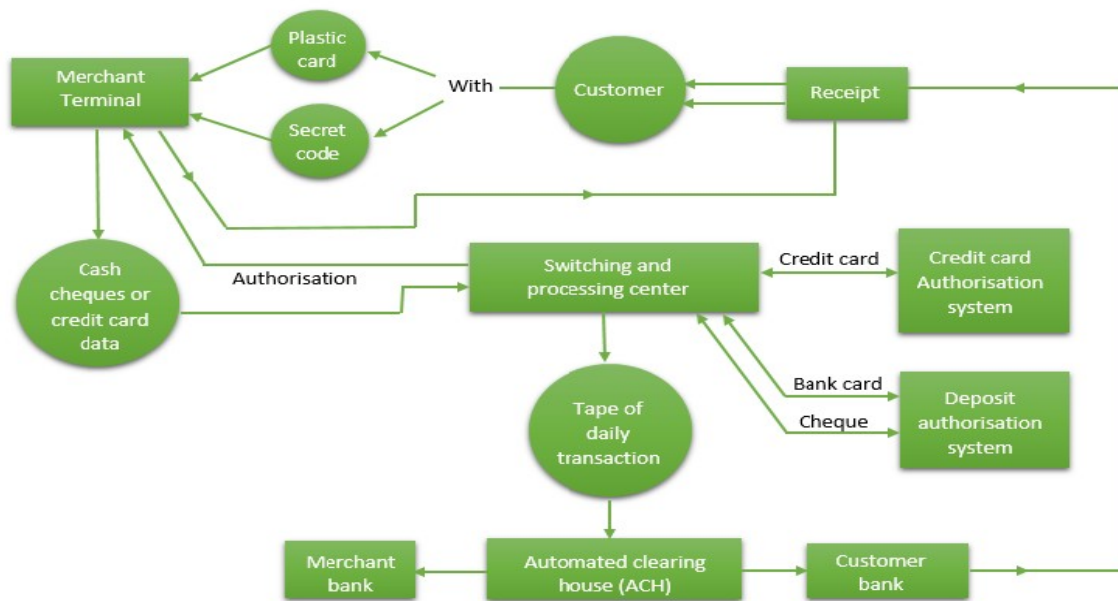
Paperless Bills :-

- Paperless Bill is a free service providing you the convenience to receive, view and pay your bill online.

- Now a days consumers are flooded with bills almost everyday like bills for medical expenses , bills of electricity , bills of housing rent ,etc.

- In paperless billing system you can see your gas and electricity bills and statements in a secure online environment.

Advantages and Disadvantages of Paperless Bills :-

Advantages:-

1. You can access your bill instantly online - no waiting for it to arrive in the post.

2. You can see previous bills and statements all in one place.

3. It saves paper, helping us be more environmentally friendly.

Disadvantages :-

1. With online billing system there is always fear of safety and security to the personal information due to the increased spywares and malwares being rampant on the internet.

Modern payment systems

Introduction

- Electronic payment systems are the alternative cash or credit payment methods using various electronic technologies to pay for products and services in electronic commerce.

- Receipt of payments is from following sources:

1. Retail customers

2. Wholesale customers

3. Various miscellaneous payments

Various Modern Payment Systems

1. PC BANKING

2. DEBIT/CREDIT CARDS

3. ELECTRONIC CHEQUES

4. MICRO-PAYMENT SYSTEMS

5. SMART CARDS

6. ELECTRONIC CASH

1.PC-BANKING

- It involves online payment transactions through internet and personal computer. It was developed after introduction of PC's and modems.

- It is a solution for both personal or banking needs without a trip to the local bank branch or the use of an ATM .

- It enables an account holder to perform real-time account activities and effectively manage financial transaction in our own schedule at any time of day or night.

- Online access to your bank account affords the customization of financial research and reports.

2.CREDIT/DEBIT CARDS

- This system started by Bank of America issued certain cards in California to select group of users to pay for products by participating merchants without cash.
- In this system , the users no longer have to carry cash to pay for a product.
- To accept these cards as payment option, one has to sign on as a merchant with the corresponding bank or credit card organization and pay a percentage of fee depending on the size and products.
- After receiving the details from the customer details like his credit card number , name , expiration date etc. the credit card must be authenticated with the credit card company so that you can receive an authorization number .This guarantees that the funds will be made available to us when we complete our deposits by ensuring that the user of the card is not over his credit limit and that the card is stolen.

3.Electronic cheques / Internet cheques

- Electronic-cheques also known as internet-cheques are used to make electronic payment between two parties through an intermediary and not very much different from the current cheque processing system . Here the cheques are generated and exchanged online.

4.MICRO-PAYMENT SYSTEMS

- A micro-payment is a very small fee paid when a visitor is sent from another website to your site and when a specific amount has been accumulated the fee is paid to the website that sent the traffic.
- This payment mechanism helps a way for you to encourage other companies to add to your links into their website.
- It is a cash payment which is made as a result of using the internet . It is based on the registration made within an organization that verifies and reports on the traffic levels between the sites.
- Since various webmasters have found out ways to defraud the system , a third party is used to track the pay per click micro-payments for the system so that the traffic generated is not a repeat traffic .
- E.g.-PayPal micropayments system , M-coin micropayment system.

5.SMART CARDS:

- A smart card is any pocket-sized plastic card that has integrated circuits embedded in it .
- Smart cards provide personal identification ,authentication ,data storage and application processing. They hold the cash ,ID information ,house and office keys , subway tokens , preference files(house temperature setting or driver seat setting etc.)and other information

- It has a microprocessor and/or a memory chip .The processor either adds or deletes or manipulates information on the card and the chip stores it permanently.
- These cards will emerge as the ultimate interface device for mobile digital economy.
- E.g. –Electronic purses , master cards etc.
- There are two types of smart cards .They are contact smart cards and contact less smart cards .

6.ELECTRONIC CASH

- Electronic cash system is a representation of monetary value equivalent to 'cash' or 'printed bank notes' except that it is transferred through networks with bits of information .
- It is preserved through public key cryptography , digital signatures and blind signatures.
- Here the user must have an e-cash software program and an e-cash bank account from which e-cash can be withdrawn or deposited.
- It is a highly secured , interoperable , accurate and retrievable method of payment system .
- The limitation of using such system is that it can't be divided into smaller amounts.

UNIT - 5

Planning e-commerce initiatives

Contents

1. Reasons for using E-Commerce Initiatives

2. Linking objectives to Business Strategies

3. Technologies offered by E-Commerce

4. E-Commerce Initiatives

5. Benefits of E-Commerce Initiatives

Reasons for using ecommerce initiatives

Improve existing customer service

As customer is the most crucial part of a business, so its progress depends upon the customers.

Improve relations with vendors & locate new vendors

Upon implementation of e-commerce company can analyse through online about all those vendors who are going to be satisfied as the best vendor for that company. As the analysis is done among all the vendors so it is understood that company will take a best decision.

Increase existing market sales:

• In order to expand our business, we need to increase our market sales.

Find new markets:

Expand sales to new areas where potential of selling goods is more.

Facilitate recruitment of new employees:

To increase our productivity , we need more manpower . More manpower means more production of commodity in a short time span.

## Linking objectives to business strategies

1.Downstream strategies:

❑ Sales Enablement :- Develop the sales tools that support the selling process.

❑ Product Launch :-Drive product launch and market-penetration process. Work with business line management of plan the launch of or implementation of the plan.

❑ Develop and drive internal product communication initiatives to raise awareness on product knowledge and positioning.

2.Upstream strategies:

❑ To perform a research about the product

❑ Build an analysis report about its sales

❑ Building strategy to improve its market value

Besides these benefits other technologies offered by ecommerce are:-

Selling and purchasing products, services and advertisements

S
A
L
E

products

Services

advertisements

P
U
R
C
H
A
S
E
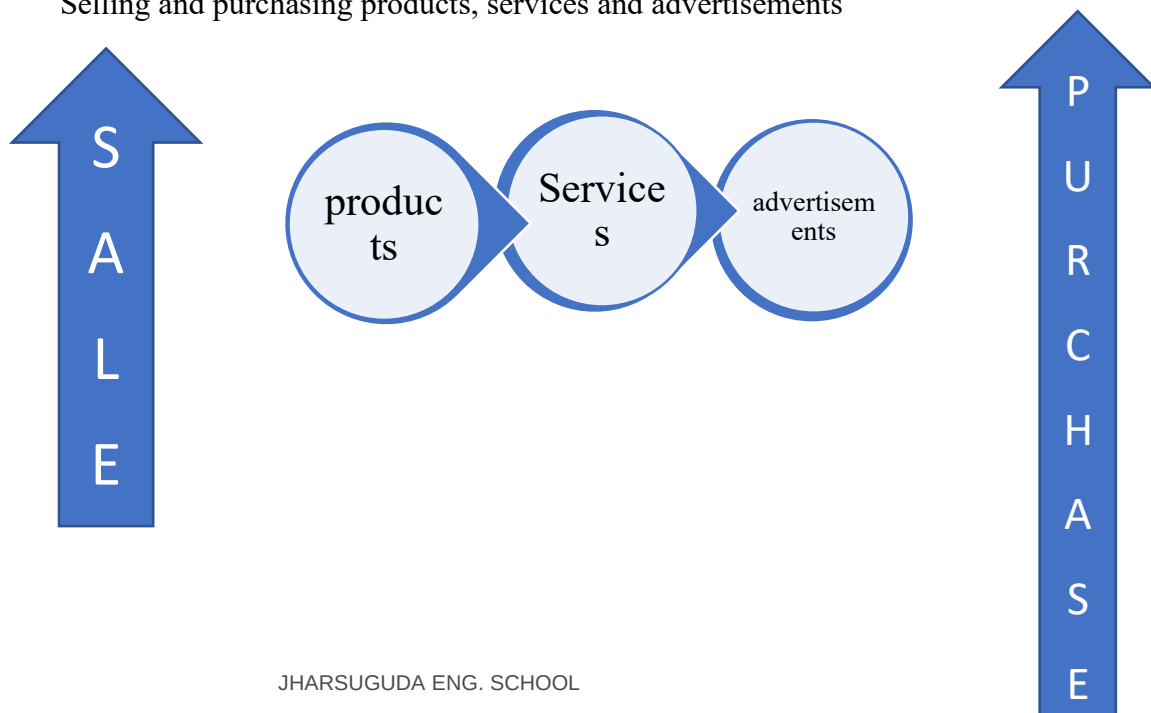
Improving customer service with after sale services and support:

Building brand name and improving current marketing programs:

Managing supply chains:

The sequence of processes involved in the production and distribution of a commodity is known as supply chain.

Ecommerce initiatives

Improve customer service

Customer satisfaction surveys, number of complaints

Enhance existing marketing programs:

Change in per-unit sales volume

Change in everything of marketing programs that is going to be enhanced for better service.

Build brands

Surveys/opinion polls that measure brand awareness must be conducted periodically.

Hold auctions

Number of auctions, all participants, number of items sold, dollar value of sales are must going to be checked timely based.

Reduce cost of after sale support

After sale support is also mandatory for making a good business organisation. If we will follow the traditional method then support service may not be as expected by customer. So it needs to be changed.

Improve supply chain

Cost, quality, and on-time delivery of purchases/services;

All these can be achieved by online implementation of them.

Measuring Cost Objectives & comparing benefits to cost

Introduction:

A cost object is a term used primarily in cost accounting to describe something to which costs are assigned. Common examples of cost objects are: product lines, geographic territories, customers, departments or anything else for which management would like to quantify cost.

What are Objectives of Cost:

Output:

The most common cost objects are a company's products and services, since it wants to know the cost of its output for profitability analysis and price setting.

Operational:

A cost object can be within a company, such as a department, production line, or process. For example, you could track the cost of designing a new product, or a customer service call, or of reworking a returned product.

Business Relationship:

A cost object can be outside of a company - there may be a need to accumulate costs for a supplier or a customer, to determine the cost of dealing with that entity. Another variation on the concept is the cost of renewing a license with a government agency.

Necessity of cost object:

❑ in order to derive pricing from a baseline cost

❑ to derive the full cost of a relationship with another entity.

A cost object may be the subject of considerable ongoing scrutiny, but more commonly a company will only accumulate costs for it occasionally, to see if there has been any significant change since the last analysis. This is because most accounting systems are not designed to accumulate costs for specific cost objects, and so must be reconfigured to do so on a project basis. An annual review is common for many cost objects.

Comparing cost & benefits:

Net Present Value (NPV):

It is defined as the sum of the present values (PVs) of incoming and outgoing cash flows over a period of time. Incoming and outgoing cash flows can also be described as benefit and cost cash flows, respectively. Projects with a NPV greater than zero are worth undertaking.

Benefits to Cost Ratio(BCR):

The BCR is the ratio of the present value of benefits to the present value of costs. The ratio should be greater than 1.0 for a project to be acceptable. For example, a BCR of 1.25 indicates that for every $1 of cost, the project will return $1.25 of benefit.

Internal Rate of Return(IRR):

IRR is the discount rate at which the present value of costs equals the present value of benefits. Alternatively, IRR is the discount rate at which NPV = 0 and BCR = 1.0. If IRR exceeds the opportunity cost of the capital, the project is considered to be economically sound and worth pursuing.

The IRR is a criteria to be used with caution because:

(i) it cannot be calculated for all projects (e.g. projects where the stream of net benefits is strictly positive for each year or projects with multiple IRR).

(ii) it is a mathematical concept and not an investment criterion for evaluating alternative cash flows. When the cash flows are irregular, with net costs occurring in the later years of the project, it will give unreliable results in the ranking of alternative options.