SYLLABUS

Paper : 20BCASD43 **Theory/Week:**4 Hours **Credits:4**	**E-Commerce**	**Hours: 40** **IA : 50** **Exam: 50**

Unit – I **8hrs**

Introduction to Electronic Commerce: The meaning, benefits, impact, Classification, application of Electronic Commerce technologies.

Electronic Commerce Business models: meaning of business model

Unit – II **8hrs**

Electronic Data Interchange: conventional trading process, meaning of EDI, building blocks of EDI system, layered architecture, value added networks, benefits and application of EDI

Electronic Commerce: Architectural framework:

Unit – III **8hrs**

Electronic Commerce: Information distribution and messaging: FTP application, Email, WWW server, HTTP, Web Servers implementation

Electronic Commerce: securing the business on Internet: Vulnerability of information on Internet, security policy, procedures and practices, site security, protecting the network

Unit – IV **8hrs**

Electronic Commerce: securing the business on Internet: transaction security, cryptography, digital signature, email security

Unit – V **8hrs**

Electronic Payment System: Introduction to payment system, Online payment system, prepaid electronic payment systems, requirement metrics of a payment system

Mobile Commerce: Introduction, Framework and models: meaning, benefits, impediments, framework

Reference Books

1.	Bharat Bhaskar, **Electronic Commerce: Framework, Technologies and Applications**, 2nd edition, McGraw Hill company, 2006
2.	David Whiteley, E-Commerce: Strategy, Technologies and Applications, Tata McGraw Hill Education Private limited, 2004
3.	Ravi Kalakota, Andrew B. Whinston, **Frontiers of Electronic Commerce**, Addison-Wesley Publications, 2000
4.	C. S. V. Murthy, **E-commerce: Concepts, Models, Strategies**, Himalaya Publishing House, 2011

CONTENTS

UNIT – IV	
E-commerce security	
6.1	Introduction on E-commerce security
6.2	Site Security Policies
6.3	Types of Security breach incidents
6.4	Protecting the network
6.5	Protecting the Network
6.6	Introduction to Cyber Security
6.7	Types of Cyber Security
6.8	Security Goals
Securing Network Transactions	
7.0	Transaction security
7.1	Threats and Attacks
7.2	Network transaction security issues
7.3	Security services
7.4	Cryptography
7.5	Digital signatures
7.6	E-mail security
Unit - V	
Electronic Payment System	
8.1	Introduction to Payment System
8.2	Online Payment Systems
8.3	Pre-paid Electronic Payment Systems
8.4	Requirement Metrics of a Payment System
Mobile Commerce - Introduction, Framework & Models	
9.1	Introduction
9.2	Benefits of Mobile Commerce
9.3	Impediments (Issues) in Mobile Commerce
9.4	Mobile Commerce Framework

TEACHING PLAN

Period	Module	Topic
1	Module 1 Introduction to Electronic Commerce	The meaning, benefits
2	Module 1 Introduction to Electronic Commerce	impact
3	Module 1 Introduction to Electronic Commerce	Classification
4	Module 1 Introduction to Electronic Commerce	application of Electronic Commerce technologies
5	Module 1 Electronic Commerce Business models	meaning of business model
6	Module 1 Electronic Commerce Business models	meaning of business model
7	Module 1 Electronic Commerce Business models	meaning of business model
8	Module 1 Electronic Commerce Business models	meaning of business model
9	Module 2 Electronic Data Interchange	conventional trading process
10	Module 2 Electronic Data Interchange	conventional trading process
11	Module 2 Electronic Data Interchange	meaning of EDI
12	Module 2 Electronic Data Interchange	building blocks of EDI system
13	Module 2 Electronic Data Interchange	layered architecture
14	Module 2 Electronic Data Interchange	value added networks
15	Module 2 Electronic Data Interchange	benefits and application of EDIElectronic Commerce
16	Module 2 Electronic Data Interchange	Architectural framework
17	Module 3 Electronic Commerce-Information distribution and messaging	FTP application, Email
18	Module 3 Electronic Commerce-	WWW server, HTTP

	Information distribution and messaging	
19	Module 3 Electronic Commerce- Information distribution and messaging	Web Servers implementation Electronic Commerce- securing the business on Internet
20	Module 3 Electronic Commerce- Information distribution and messaging	Vulnerability of information on Internet
21	Module 3 Electronic Commerce- Information distribution and messaging	security policy
22	Module 3 Electronic Commerce- Information distribution and messaging	procedures and practices
23	Module 3 Electronic Commerce- Information distribution and messaging	site security
24	Module 3 Electronic Commerce- Information distribution and messaging	protecting the network
25	Module 4 Electronic Commerce- securing the business on Internet	transaction security
26	Module 4 Electronic Commerce- securing the business on Internet	transaction security
27	Module 4 Electronic Commerce- securing the business on Internet	cryptography
28	Module 4 Electronic Commerce- securing the business on Internet	cryptography
29	Module 4 Electronic Commerce- securing the business on Internet	digital signature
30	Module 4 Electronic Commerce- securing the business on Internet	digital signature

31	Module 4 Electronic Commerce-securing the business on Internet	email security
32	Module 4 Electronic Commerce-securing the business on Internet	email security
33	Module 5 Electronic Payment System	Introduction to payment system, Online payment system
34	Module 5 Electronic Payment System	prepaid electronic payment systems
35	Module 5 Electronic Payment System	requirement metrics of a payment system
36	Module 5 Electronic Payment System	Mobile Commerce-Introduction
37	Module 5 Electronic Payment System	Framework and models-meaning
38	Module 5 Electronic Payment System	benefits
39	Module 5 Electronic Payment System	impediments
40	Module 5 Electronic Payment System	framework

UNIT – I

INTRODUCTION TO ELECTRONIC COMMERCE

1.1 INTRODUCTION

The term Electronic commerce (E-commerce) can be defined as a technology used for performing a variety of market transactions like delivery of information, products, services, and payments enabled by information technology and conducted over communication networks or other means.

The emergence of the internet as a vast public network with millions of people connected online has given rise to a new interactive marketplace for buying and selling. Thus, for some electronic commerce simply means the capability to buy and sell goods, information and services online through the public networks.

There are 5 phases or elements in an E-Commerce Market

- Information Exchange:
- Contract and Order:
- Shipment and Payment:
- Customer Service and
- Marketing

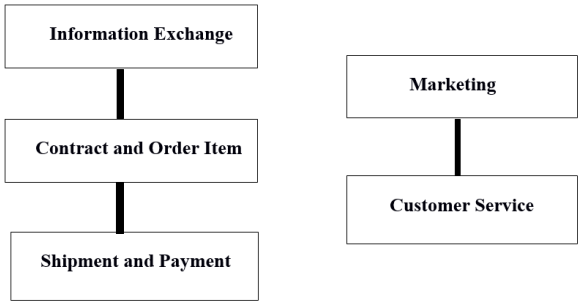


Fig 1.1 E–Commerce Market Elements

- **Information Exchange:** Here the e-commerce system may include banner advertisements, details of products or services, and electronic catalogs providing information on pricing, quality, delivery and payment terms
- **Contract and Order:** In this phase, the order is placed and item is contracted by the customer.
- **Shipment and Payment:** This stage follows after the exchange of values, which may involve physical or electronic shipment. Payment in E-commerce can be done through credit cards, digital cash, or any other electronic payment systems.

In addition to these 3 main elements, there are two more supplementary elements-

- **Customer Service:** If some of the item parts being delivered are faulty or missing, the

customer can ask for a customer service for the product or replacement of that part or item.

- **Marketing** deals with activities like advertising of the product, product promotion, etc. The marketing element utilizes the data generated by customer support, along with any other feedback or feature references. These elements relate to each other in a circular fashion that over a period of time may promote further economic activity.

Key areas of a typical e-Commerce process flow include:

- Receiving orders from your e-Commerce system
- Processing order information
- Shipping

Examples of E-Commerce

- **Online Shopping**

Buying and selling goods on the Internet is one of the most popular examples of e-Commerce. Sellers create storefronts that are the online equivalents of retail outlets. Buyers browse and purchase products with mouse clicks. Though Amazon.com is not the pioneer of online shopping, it is arguably the most famous online shopping destination.

- **Electronic Payments**

When you are buying goods online, there needs to be a mechanism to pay online too. That is where payment processors and payment gateways come into the picture. Electronic payments reduce the inefficiency associated with writing and mailing checks. It also does away with many of the safety issues that arise due to payment made in currency notes.

- **Online Auctions**

When you think online auction, you think eBay. Physical auctions predate online auctions, but the Internet made auctions accessible to a large number of buyers and sellers. Online auctions are an efficient mechanism for price discovery. Many buyers find the auction shopping mechanism much interesting than regular storefront shopping.

- **Internet Banking**

Today it is possible for you to perform the entire gamut of banking operations without visiting a physical bank branch. Interfacing of websites with bank accounts, and by extension credit cards, was the biggest driver of e-Commerce.

- **Online Ticketing**

Air tickets, movie tickets, train tickets, play tickets, tickets to sporting events, and just about any kind of tickets can be booked online. Online ticketing does away with the need to queue up at ticket counters.

Electronic Commerce under different perspectives:

Let's see how Electronic Commerce (EC) is defined under each perspective.

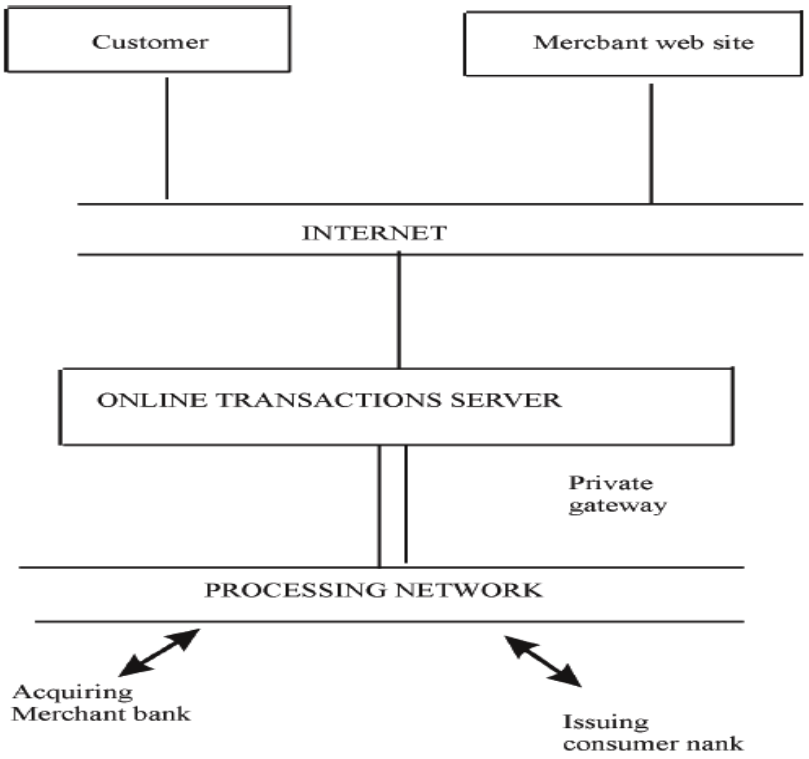
1. ***Communications Perspective:*** EC is the delivery of information, products /services, or payments over the telephone lines, computer networks or any other electronic means.
2. ***Business Process Perspective:*** EC is the application of technology toward the automation of business transactions and work flow.
3. ***Service Perspective:*** EC is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.
4. ***Online Perspective:*** EC provides the capability of buying and selling products and information on the internet and other online services.

E- Commerce in Action

How E-Commerce Works???

The consumer first moves through the internet to the merchant's web site. At the web site, the consumer is briefly given an introduction to the product or services the merchant offers. It is at this point that the consumer makes the decision to visit the web store by clicking on a link or button located on the web page (e.g., Buy Now, Shop Online, or an image of a shopping cart button are common entry points into a web store). After choosing to visit the web store, the consumer is typically connected to an online transaction server located somewhere else on the internet which runs software commonly referred to as a shopping cart application. The shopping cart application has been setup by the merchant to display all products and services offered, as well as calculate pricing, taxes, shipping charges, etc.

From there, the consumer decides that he wants to purchase something, so he enters all pertinent credit card information and a sales order is produced. Depending on the e-Commerce implementation, the sales order can now take two totally different paths for confirming to the consumer that the order is officially placed.



Scenario 1

The consumer's credit card information goes directly through a private gateway to a processing network, where the issuing and acquiring banks complete or deny the transaction. This generally takes place in no more than 5-7 seconds and the consumer is then informed that the order was received, the credit card was authorized, and that the product will ultimately be shipped.

Scenario 2

The consumer's entire order and credit card information is electronically submitted back to the merchant's server (usually via email, FTP, or SSL connection) where the order can be reviewed first and then approved for credit card authorization through a processing network. The consumer then receives an email shortly afterward, confirming the order being received, the credit card being authorized, and status on when the product will exactly be shipped.

In both scenarios, the process is transparent to the consumer and appears virtually the same. However, the first scenario is a more simplistic method of setting up a shopping cart application and does not take into consideration any back office issues that may delay shipment (i.e., items out of stock, back orders, orders submitted after office hours or during holidays, etc.). Manage More's e-Commerce Manager relies on the second scenario to handle all of its e-Commerce orders. This second scenario keeps the consumer accurately informed throughout the entire ordering process.

Top-Level e-Commerce Process Flow

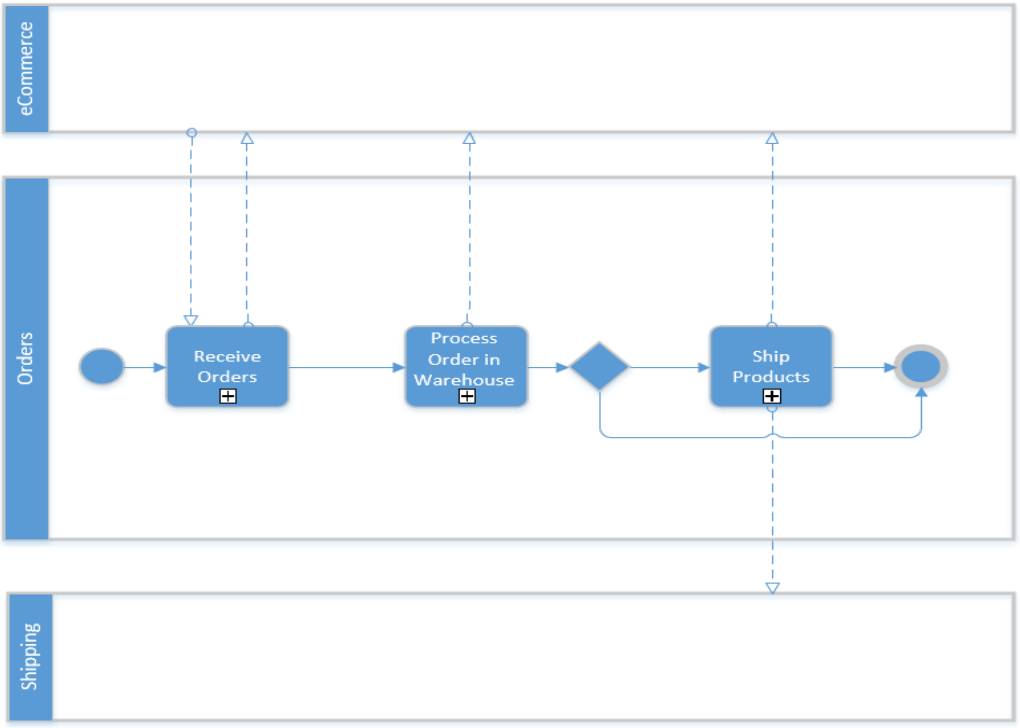


Diagram: Overview of a typical e-Commerce process flow

Unless you are already automating your e-Commerce processes, managing e-Commerce orders is a manual process. Employees have to log in and out of different business systems and databases, which is both time-consuming and prone to errors.

Each top-level process highlighted below holds a number of additional subprocesses (+). For example, when a sales order hits your back office operations employees have to manually process the information into your business software. This can result in administration errors and create process bottlenecks further down the line. In an automated process employee intensive administration tasks are removed.

At the top level of an e-Commerce process flow, the following can be easily identified:

- Customer places an order in your e-Commerce system
- Order details are extracted from your e-Commerce system and entered into your business software
- Order is passed to the warehouse to be processed
- Order is placed for fulfilment

Sub process: Receiving Orders

When a customer places an order within your e-Commerce system the order details need to be extracted and placed into your business software. Manually dealing with information held within a sales order can detract from the businesses planned objectives. Data entry errors can surface, employee efficiency is reduced and order processing costs increase.

The process of receiving the order is mapped below.

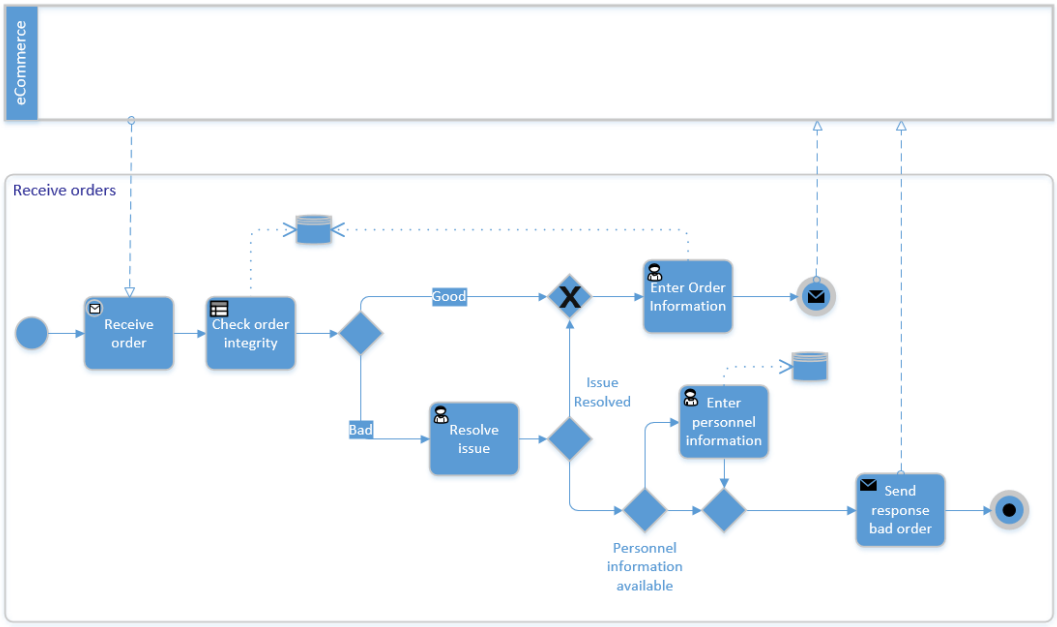


Diagram: Receiving orders from an e-Commerce system and placing into business software

- Sales order details are manually extracted from your e-Commerce system. Information includes customer information, description and ID of product ordered, payment details and transaction ID
- Employee manually checks sales order data for a correlation with your business rules e.g. full address, contact details, products ordered
- Employee manually enters order and customer details into your business software
- Employee manually creates and sends an order received notification to the customer
- If an employee identifies any anomalies they will need to contact the customer to resolve the issue
- If an issue cannot be resolved the employee may have to manually cancel the order
- Order is passed to warehouse for processing

How automation can help this process?

By automating this process the employee is removed from the scenario. If required, orders can be pulled on a timed or scheduled basis e.g. every 15 minutes. Orders are automatically entered into your business software and the customer receives and automated

order confirmation notification. For a detailed overview of automated e-Commerce processes.

Sub process: Processing an Order in the Warehouse

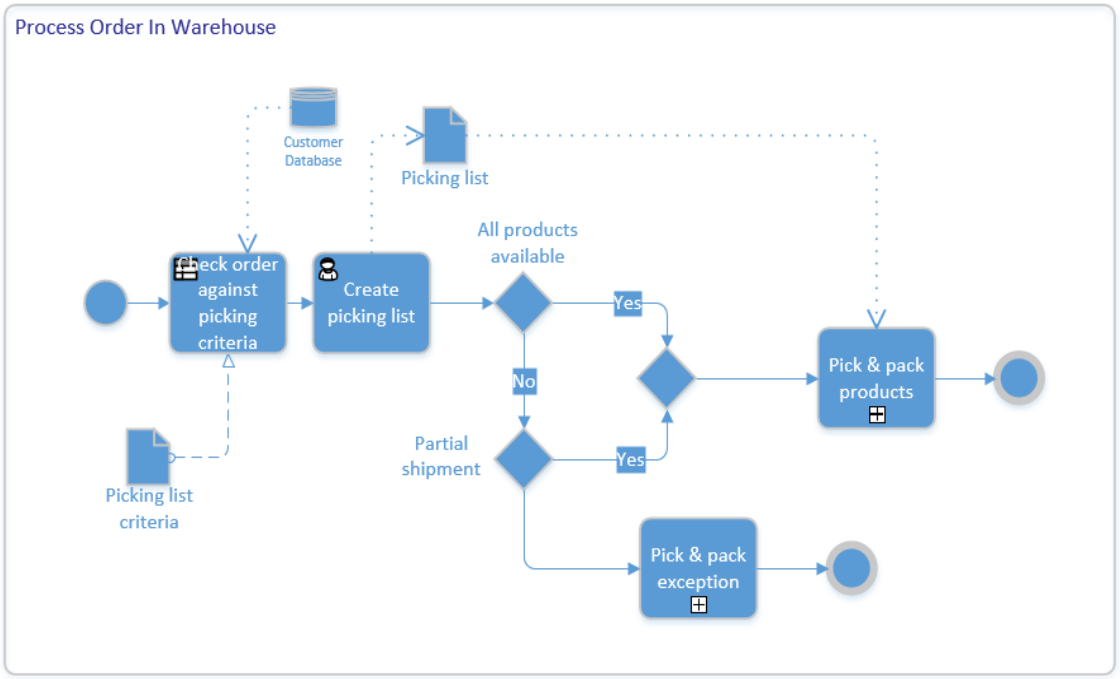


Diagram: Processing orders in the warehouse

- Employee notifies warehouse of an order that needs to be processed
- Employee manually checks the order against pick list criteria e.g. stock availability, item location in warehouse etc.
- Employee creates and prints pick list
- If products are in stock and available, the order is picked and packed
- Order is now ready for the shipping process

How automation can help this process?

An automated process will reduce employee time in cross-referencing your business software for stock availability and product location. It will dynamically automate the creation and printing of your pick lists. For a detailed overview of automated e-Commerce processes.

Sub process: Processing an Order for Shipping

Once an order has been processed in the warehouse it is now ready to be passed to shipping for fulfilment with a courier. Here, your business rules will determine which shipping

route the employee chooses. Package data, such as weight, size, destination and costs, needs to be obtained. An employee will also need to manually print the shipping labels and contact the courier for fulfilment.

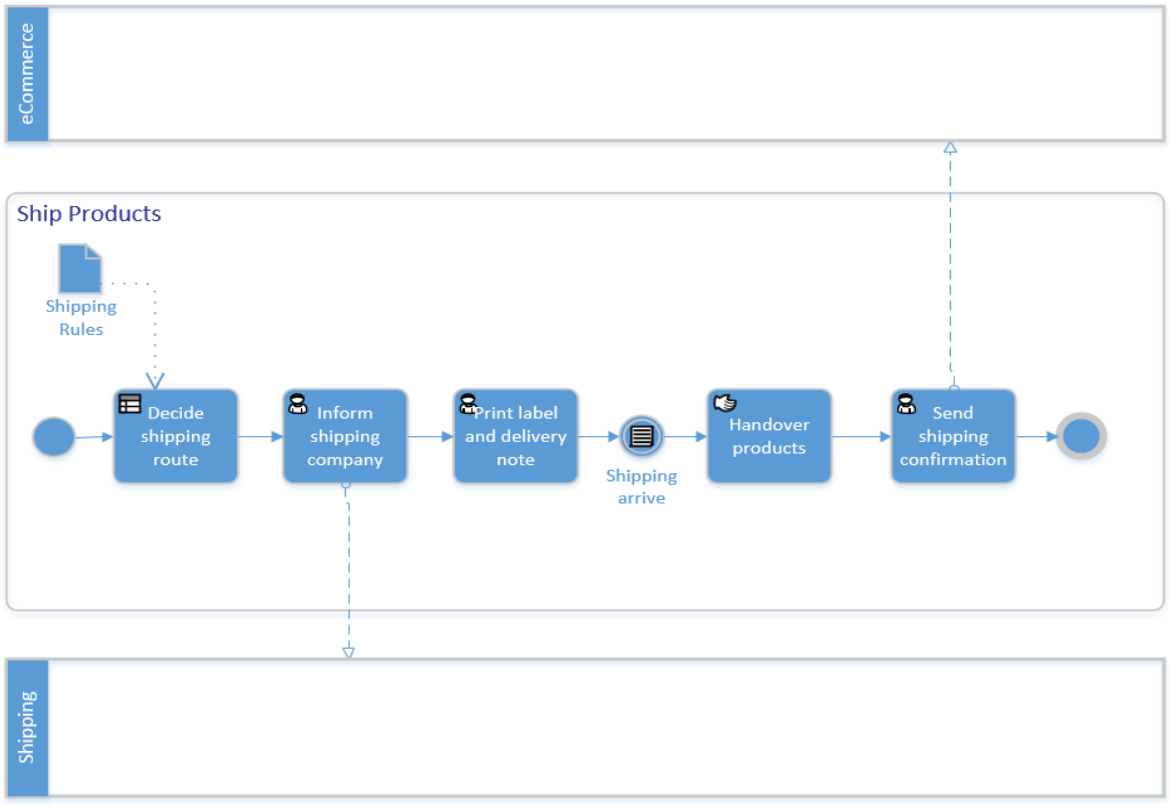


Diagram: Shipping products for fulfilment

- Employee enters package data, such as weight, size and destination into your courier provider system
- Employee prints shipping labels and delivery notes
- Shipping confirmation sent to customer
- Employee may or may not update your business software with tracking numbers
- Order handed over to courier for fulfilment

How automation can help this process?

An automated fulfilment process will remove the manual administration in this process as all package data and courier details will be in your business software. Your business systems will be integrated with your courier service provider's solution, enabling them to 'talk to each other'. An automated process will also provide you with the ability to automatically print shipping labels. The customer will receive an automated 'dispatched' notification, and tracking details will automatically synchronise with your business software. For a detailed overview of automated e-Commerce processes.

1.2 BENEFITS OF E-COMMERCE

- Reaching a wider market segment irrespective of rich, poor, young, old, etc. Only thing is you should have an internet connection
- Distances do not matter in carrying out trade. You can reach the customer wherever he is located in the world, any time you want
- Availability of items 24 hours a day, 7 days a week and 365 days a year.
- Setting up an E-commerce website is cheaper compared to having a brick and mortar retail outlet.
- Wider choice for the customers
- Flexibility to add & remove items from the list easily
- Reduction in human errors due to automation
- Exposure to previously untapped market segments
- Availability of friendly advice
- Reduction in order processing cost & time
- Faster fund transfer
- Reachability of producer with consumer directly

Benefits to Organizations

- Electronic commerce expands the marketplace to national and international markets. With minimal capital outlay, a company can easily and quickly locate more customers, the best suppliers, and the most suitable business partners worldwide.
- Electronic commerce decreases the cost of creating, processing, distributing, storing, and retrieving paper-based information. For example, by introducing an electronic procurement system, companies can cut the purchasing administrative costs by as much as 85 percent.
- Ability for creating highly specialized businesses. For example, dog toys which can be purchased only in pet shops or department and discount stores in the physical world, are sold now in a specialized
- E-commerce helps organizations to reduce the cost to create process, distribute, retrieve and manage the paper based information by digitizing the information.
- E-commerce improves the brand image of the company.
- E-commerce helps organization to provide better customer services.
- E-commerce helps to simplify the business processes and makes them faster and efficient.

- E-commerce reduces the paper work.
- Electronic commerce lowers telecommunications cost-the Internet is much cheaper than VANs.
- Other benefits include improved image, improved customer service, newfound business partners, simplified processes, compressed cycle and delivery time, increased productivity, eliminating paper, expediting access to information, reduced transportation costs, and increased flexibility.

Benefits to Consumers

- Electronic commerce enables customers to shop or do other transactions 24 hours a day, all year round, from almost any location.
- Electronic commerce provides customers with more choices; they can select. Electronic commerce frequently provides customers with less expensive products and services by allowing them to shop in many places and conduct quick comparisons.
- In some cases, especially with digitized products, EC allows quick delivery.
- Customers can receive relevant and detailed information in seconds, rather than days or weeks.
- Electronic commerce makes it possible to participate in virtual auctions.
- Electronic commerce allows customers to interact with other customers in electronic communities and exchange ideas as well as compare experiences.
- Electronic commerce facilitates competition, which results in substantial discounts.

Benefits to Society

- Electronic commerce enables more individuals to work at home and to do less travelling for shopping, resulting in less traffic on the roads and lower air pollution.
- Electronic commerce allows some merchandise to be sold at lower prices, so less affluent people can buy more and increase their standard of living.
- Electronic commerce enables people in Third World countries and rural areas to enjoy products and services that otherwise are not available to them.
- Electronic commerce facilitates delivery of public services, such as health care, education, and distribution of government social services at a reduced cost and/or improved quality. Health-care services, for example, can reach patients in rural areas.

Drawbacks of E-Commerce

- Inability to touch & feel merchandise

- Computer systems are not 100% safe, someone may hack your private data
- All customer segments cannot be reached over online
- Access to internet is yet to reach all the customers
- Trust building with customers with only web presence is difficult
- Lack of social contacts

1.3 CLASSIFICATIONS OF E-COMMERCE

Electronic commerce has been classified in 5 main categories:

- Business-to-Business (B2B)
- Business-to-Consumer (B2C)
- Consumer-to-Business (C2B)
- Consumer-to-Consumer (C2C)
- Business-to-Employee (B2E)

Sometimes the government may operate with its own set of rules and thus at times the Business-to-Government (B2G) category is also included.

Business-to-Business (B2B) E-Commerce

Business-to-Business electronic commerce facilitates **Inter-organizational** interaction and transaction. This type of electronic commerce requires two or more business entities interacting with each other directly, or through an intermediary. The intermediaries in Business-to-Business EC may be market makers and directory service providers, who assist in matching buyers and sellers and striking a deal.

Business to Business transaction between a vendor and a purchaser of goods will be as under:

1. A purchase order (P.O) document is entered in the keyboard of a PC by the customers purchase office and sent by e-mail to the vendor in a standard format for the purchase order through Electronic Data Interchange (EDI) standard.
2. The P.O. is stored in the vendor data base and is acknowledged electronically through EDI. No manual transaction of entering the PO at the vendor's side.
3. The vendor physically (in a rail or truck) dispatches the items and the delivery note is sent through EDI standard. (No need of re-entering delivery note manually). Delivery note is compared with P.O. again through EDI. If no match found, a discrepancy note is released electronically (through EDI).
4. The items received at the customer end will have a printed delivery note accompanying them and is sent to the inspection office at customer’s end which physically inspects items received and compares with the delivery note received electronically.

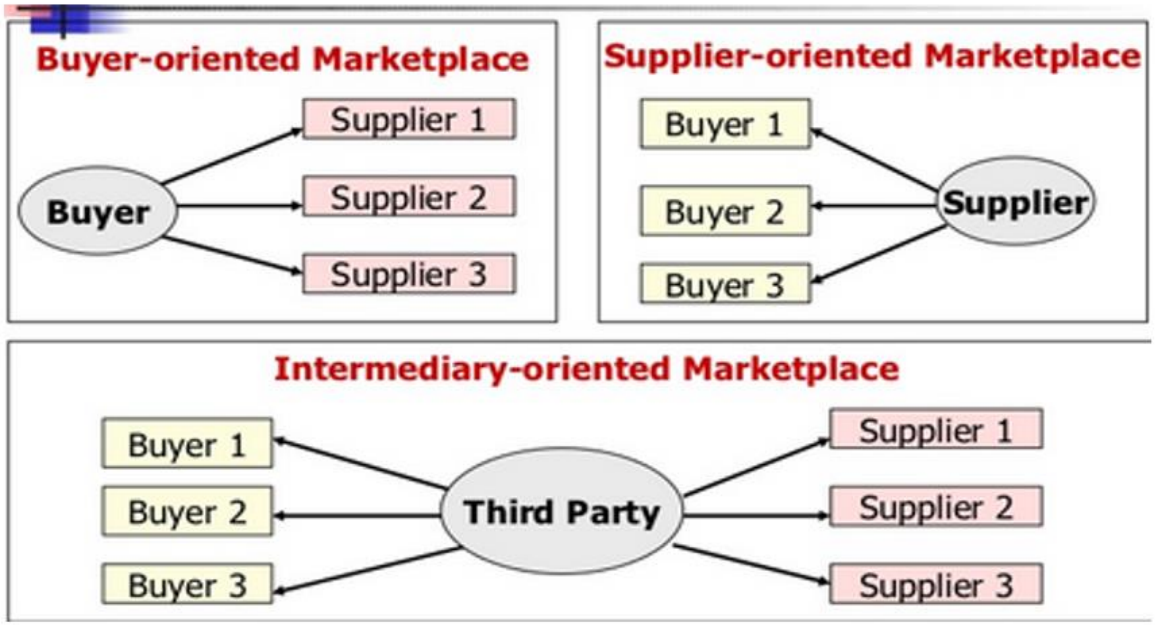
5. The stores office computer updates the inventory automatically using the note sent by Inspection office.
6. The accounts office makes the payment for the items accepted through Electronic Funds Transfer (EFT).Its banker is informed electronically to debit its account by the specified amount and the same is to be credited to the vendor's bank account.

The business application of B2B electronic commerce can be utilized to facilitate almost all facets of interactions among organizations, such as supplier management, inventory management, channel management, distribution management, order fulfilment and delivery, and payment management. The B2B electronic commerce can be a supplier-centric, buyer-centric, or an Intermediary-centric.

Architectural Models

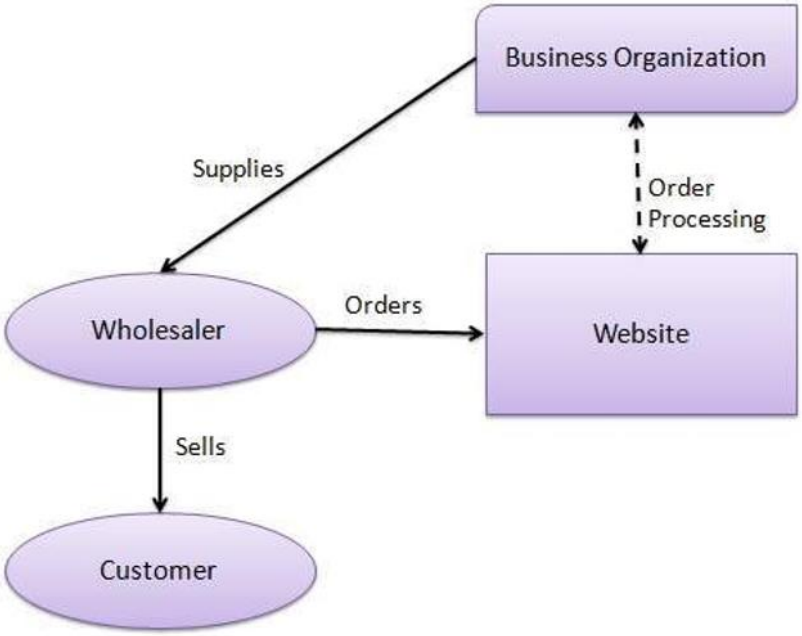
Following are the architectural models in B2B e-commerce −

- **Supplier Oriented marketplace** − in this type of model, a common marketplace provided by supplier is used by both individual customers as well as business users. A supplier offers an e-stores for sales promotion.
- **Buyer Oriented marketplace** − in this type of model, buyer has his/her own market place or e-market. He invites suppliers to bid on product's catalog. A Buyer company opens a bidding site.
- **Intermediary Oriented marketplace** − in this type of model, an intermediary company runs a market place where business buyers and sellers can transact with each other.



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.

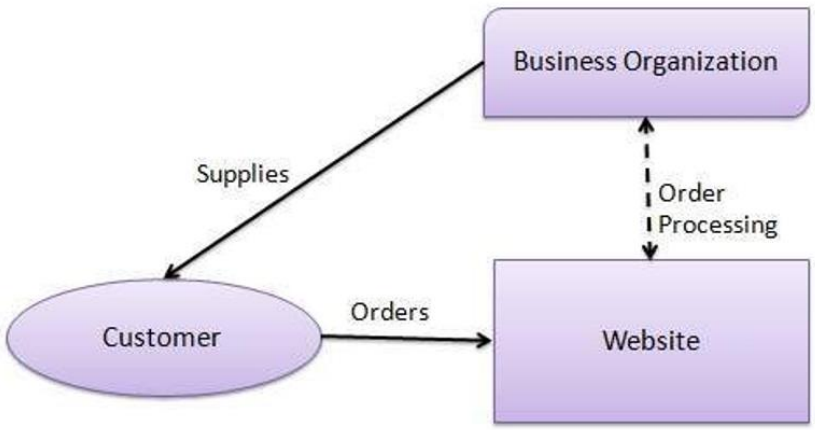


Business-to-Consumer (B2C) E-Commerce

Business-to-Consumer (B2C) electronic commerce offers consumers the capability to browse, select, and buy merchandise online, from a wider variety of sellers and at better prices. The two or more entities that interact with each other in this type of transaction involve one selling business and one consumer. The selling businesses offer a set of merchandise at given prices, discounts, and shipping and delivery options. In this type of electronic commerce the sellers and consumers both benefit through the round the clock shopping accessibility from any part of the world, with increased opportunity for effective direct marketing, customizations, and online customer service.

The application of electronic commerce in the retailing segment has seen it evolve from an online version of catalog selling to accepting orders and payments online and translating zero inventories into huge discounts on the prices of items. The user makes payments for the purchased item using digital cash, credit cards or using the newest form of payment - cash on delivery.

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**.**



The B2C model of electronic commerce transaction is ideally suited for the following types of merchandise:

1. Goods that can be easily transformed into digital format, such as books, music clips and videos, and software packages.
2. Items that follow standard specifications, like printer ribbons, ink cartridges etc.
3. Highly rated branded items or items with return security: such as Dell and Compaq computers, electronic gadgets from Sony, etc.
4. Items sold in packets that cannot be opened even in physical stores, e.g., Kodak film rolls.
5. Relatively cheap items where savings outweigh risks.
6. Items that can be experienced online, such as music, videos etc.

The B2C electronic commerce opportunity has been utilized by three types of businesses- Channel enhancement, On-line internet-based stores, and small businesses trying to surpass entry barriers.

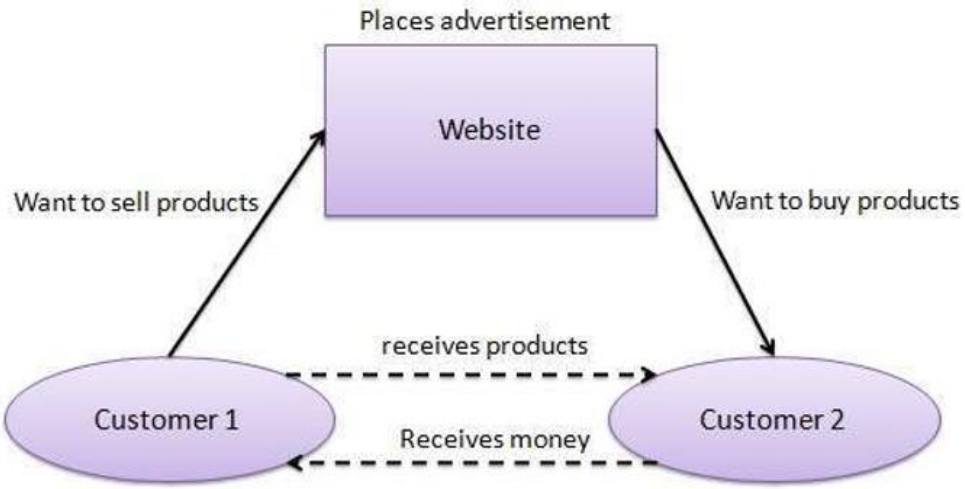
Existing businesses may use it for expanding the market space and revenues by utilizing the internet as new channel to do business with customers, where customers could place orders for goods and services online. Also, existing consumer merchandisers with established store channels adopt B2C electronic commerce to augment sales through a new channel, as well as to make it easier to reach out to global customers. Some examples of B2C e-Commerce sites are www.dell.com, www.flipkart.com, etc.

Consumer-to-Consumer (C2C) E-Commerce

Consumer-to-consumer (C2C) electronic commerce gives the opportunity for consumers to transact goods or services with other consumers present on the internet. The items like craft, merchandise and similar items that are normally sold through 'flea' markets or bazaars are sold in C2C websites, where individuals sell their goods to other individuals at market determined prices. To many others, it is defined as a financial interaction between non-business entities using the web.

The C2C in many situations uses models that exchange systems with a modified form of deal making. For deal making purposes a large virtual consumer trading community is developed. The customer operates by the rules of this community to compete, check and decide his own basic selling and/ or buying prices. Traditionally, C2C electronic commerce has been conducted through both trading forums and intermediaries such as auctions, classified advertisements, and collectible shows.

It gives small firms and individuals the same opportunity as multi-national corporations. As a result, many individuals established online organizations that encouraged and assisted commerce between consumers. EBay's auction service is a great example of C2C e-com where person-to-person transactions take place every day. Other examples include sites like OLX.in, Quikr.com etc. where users can sell their second-hand items to other users online.



Consumer-to-Business (C2B) E-Commerce

Consumer-to-Business (C2B) e-commerce is also called demand collection model. The C2B model involves a transaction that is conducted between a consumer and a business organization. It is similar to the B2C model, however, the difference is that in this case the consumer is the seller and the business organization is the buyer. In this kind of a transaction, the consumers decide the price of a particular product rather than the supplier. It enables buyers to name their own price, often binding, for a specific good or services generating demand. A consumer posts his project with a set budget online and companies review the customers' requirements and bids out the project. Then the customer will review the bids and selects the company that will complete the project. Example: Stock market.

Business-to-Employee (B2E) E-Commerce

It is also called as **Intra-organizational** Electronic Commerce. Intranets are corporate networks that utilize internet technology but limit the access only to the internal members of an organization. Typically, they are built by securing the network from the global internet, through a firewall that limits access to internal authorized members only. The internet has

provided users equipped with a browser, the means to communicate with everyone on the web, irrespective of what platform they have. The intranets are deployed to incorporate these advantages of the web into the information systems of the organization.

These applications enable managers to communicate with employees using emails, video concerning and bulletin boards. The goal is to increase the flow of information, resulting in better informed employees. These applications enable companies to organize, publish and spread human resources manuals, product specifications and meeting minutes in their bulletin board. The flow of information between the production and sales forces, and between the firms and customers can also be published here.

Thus efficient management of the intellectual assets and resources of a company is crucial for creating better business value and gaining competitive advantage. The intranet based business-to-employee applications are often used for implementing improved employee relationship management initiatives.

1.4 APPLICATIONS OF E-COMMERCE TECHNOLOGIES

1. Electronic Auctions

Auctions have been a well-established market mechanism for trading items at a market negotiated price, based upon demand and supply. The internet has added a new dimension by creating an online mechanism for implementing the auction process. Traditional auctions had limited participation of people who turned up at the place of auction. Today, the same auction mechanisms can be implemented using electronic commerce technologies, allowing people connected through the internet to bid. Electronic auctions potentially encourage greater participation as internet users can connect to a web site- hosting an auction and bid for an item.

2. Electronic Banking

Using E-commerce technologies, bank user records and all financial transactions can be done using the respective Bank's website. The user can also use the website to balance his check book, summarize credit card purchases, track stocks and other investments. With the wide availability and access to internet, electronic banking empowers activities such as accessing their accounts, carrying out debit and credit transactions, transfer funds, pay bills, review account history etc. ICICI bank, Citibank, HDFC bank, SBI and other leading banking companies have been offering Internet banking services for the past few years.

3. Electronic Searching

The complete functionality offered by a telephone directory service provider can be offered through a single web interface using HTTP server, where a user can search for any details like products, person, place or any other information on the web. Companies like Google.com, Bing.com, Whowhere.com and Altavista.com not only serve the purpose but also contains personal pages, business pages, and general information on almost each and every topic and subject. In addition to that, it can provide a lot more relevant information including travel direction and a map of the vicinity.

4. Education and Learning

The internet today is widely used as a delivery vehicle for training and learning as well. The web technology provides a uniform delivery mechanism for textual, multimedia and animated contents called as **e-Learning,** with the concept of delivering training over the internet. E-Learning has already taken powerful roots and is emerging most predominantly in the information technology universe, as IT professionals are more comfortable working with the new technology and have access to high speed internet connections for the fast transmission required for media rich lessons.

Training and continuing education in the field of information technology has evolved from spending hours outside an office in a classroom, or hours in front of a computer, dull presentations to a flexible anytime anywhere convenience mode. Today internet is empowering professionals with flexible training and customized learning, with live and virtual classrooms over the web through innovative electronic training technologies, flexible delivery methods, engaging multimedia, and live audio.

With the growth of internet technologies and the bandwidth availability today internet based training is capable of providing content in multiple formats like textual, audio, video and other emerging formats. E-Learning has matured to the extent that course developers, rather than being preoccupied with the software and hardware behind the scenes, can pay more emphasis on providing students a better experience than they might have had even with a traditional instructor led class in a brick and mortar environment.

With e-learning, we are able to move beyond the novel concept that the person teaching them is not physically in the same building as they are. The focus in such an e-learning environment is on engaging them and keeping the learners engrossed in the information being conveyed. The key benefit of e-learning is that it allows professionals to take classes according to their time convenience who may have problems with their work schedules and couldn't attend regular class room hours. Apart from that it saves time on commuting to the traditional brick-and-mortar training classes and it is also difficult to be away from the office for long periods. The online instructor, who is a real teacher, can interact and explain concepts and clear doubts of anyone attending a course, no matter where the students are located, as long as they are sitting in designated classrooms or connected online.

Marketing

Traditional marketing practices are being carried upon by companies using e-commerce technologies because it faces following major challenges:

- **Higher Costs:** The Company incurs costs in producing brochures and product data sheets and in shipping and mailing them to customers.
- **Hit Ratio:** Direct mail, even in targeted market places, suffers from extremely low response rates.
- **Time Intensive**: Marketing tasks are often time constrained, leading to intense time pressure in organizing the activity. The preparation of an advertisement or a marketing communication brochure may require several rounds of revisions, leading to delays.

Internet advertising offers the following salient advantages:

- **Cost and Time Savings:** Catalogues, brochures, product specifications prepared in the electronic form and delivered through the internet offer huge savings in copy editing, printing, packaging and shipping costs and updating as and when required. Also, it cuts the time to put the information in the customer's hands and up to date information is available to customers worldwide, continuously through the reach of the internet.
- **Lower Barrier to Entry:** The size of business, location of business, and the brick and mortar infrastructure does not matter when you are present on the internet. It offers equal opportunities to one and all by lowering barriers to access the marketplace.
- **Interactivity and Information Richness**: Marketing teams can develop interactive rich media based brochures, product specifications, and 3-D views of products and operating scenarios, and place them on the web site. Analytical buyers can use the information to get enough information to make an informed decision through interaction with the site.
- **Alternate Channel:** For existing businesses, electronic marketing opens up a new channel that gives customers the opportunity to browse, collect information, analyze and then chose the standard product or customize it to their taste (e.g., color, size, shipping method) and then place the purchase order.

Traditional vs. Electronic Commerce

Comparison Feature	***Traditional commerce***	***E-commerce***
Definition & Meaning	Traditional commerce focuses on the exchange of products and services through personal interactions	E-commerce focuses on the exchange of goods and services via the Internet
Accessibility	Limited to several hours during the day	Can be accessed anytime 24/7
Customer Interface	Customers interact with business face-face	Customers use computing devices to access and interact with business
Business Scope	Geographically limited to business location	Global business scope
Mode of Delivery	Instant	Time-consuming
Transaction Processing	Manual	Automatic
Product Physical Inspection	Can be done before purchase	Cannot be done before purchase

Maintenance	Easier to maintain this as the only warehouse is enough to store the goods.	It is cost effective as display and showcase of the products are required to attract the customers.

Main goals of E-Commerce:

- **Wider reach:** E-Commerce provides a platform for business to operate freely and reach a wider audience.
- **Not bound by limitations**: E-Commerce should allow users operate without "this site" the limitations of space, time and locations. Customers should be able to interact and transact with lease hassles.
- **Customer Experience**: It should provide users a faster and convenient mode of shopping. Some people consider shopping as a social experience and might not like online shopping though it has its comforts. E-Commerce experience should be improved with intuitive and good interface so that users enjoy online shopping.
- **New revenue collecting techniques**: We already know about the traditional techniques of revenue collection, for example, payment upon receipt, advance payment, and so on. At present, electronic commerce supports more improved methods of revenue collection. For example, an information product service provider will allocate the product broadly and then charge on a usage basis - which means charging the customer only when the information is used.
- **Transaction devices**: It is necessary that e-commerce adapts the technologies and devices required for reaching and maintaining the mass market.
- **Security**: e-Commerce sites, services, and payment accesses should be secure so that customer feels secure with transactions.

MULTIPLE CHOICE QUESTIONS

Questions for Remembering

a. Can you name which phase of E-commerce system has replacement of parts or item?

A. Information Exchange

B. Contract and Order

C. Shipment and Payment

D. **Customer Service**

b. Can you name which perspective says that EC is the application of technology toward the automation of business transactions and work flow.

A. Communications Perspective

B. **Business Process Perspective**

C. Service Perspective

D. Online Perspective

c. What is the full form of B2B?

A. **Business to Business**

B. Bank to Bank

C. Bank to business

D. Business to Bank

d. Can you name Which E-commerce supports Inter-organizational interaction.

A. **Business-to-Business (B2B)**

B. Business-to-Consumer (B2C)

C. Consumer-to-Business (C2B)

D. Consumer-to-Consumer (C2C)

e. Can you name which e-commerce is also called demand collection model?

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. **Consumer-to-Business (C2B)**

D. Consumer-to-Consumer (C2C)

f. Can you name Which E-commerce supports Intra-organizational interaction.

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)
C. Consumer-to-Business (C2B)
D. **Business-to-Employee (B2E)**

g. What is the Full form of VAN?
   A. **Value added Network**
   B. Value area Network
   C. Validation added network
   D. Validation area network

h. Define Electronic Commerce.
   A. Commerce of electronic good
   B. Commerce which depends on electronics
   C. Commerce which is based on the use of internet
   D. **Commerce which is based on transactions using computers connected by telecommunication network**

i. What is the Full form of EDI?
   A. **Electronic Data Interchange**
   B. Electronic Digital Interchange
   C. Electronic Data Issue
   D. Electronic Digital Issue

j. Can you name, EDI is most commonly used in which type of E commerce.
   A. **B2B**
   B. B2C
   C. C2C
   D. C2B

k. What is the Full form of EFT?
   A. **Electronic Fund Transfer**
   B. Electronic Faster Transfer
   C. Electronic Fund Technology
   D. Electronic Fast Technology

l. Can you name under which E-commerce Stock Market comes.

A. B2B

B. B2C

C. C2C

D. **C2B**

m. Can you name which among the following is not part of B2B architectural model.

A. Supplier Oriented marketplace

B. Buyer Oriented marketplace

C. Intermediary Oriented marketplace

D. **Time Oriented marketplace**

Questions for Understanding

n. Can you clarify, Banner advertisements are included in _____ phase of E-commerce system.

A. **Information Exchange**

B. Contract and Order

C. Shipment and Payment

D. Customer Service

o. Can you clarify this, EC is the delivery of information, products /services, or payments over the telephone lines, computer networks or any other electronic means, which of the following perspective define this?

A. **Communications Perspective**

B. Business Process Perspective

C. Service Perspective

D. Online Perspective

p. What do you think, E-bay is an example of which type of E-commerce.

A. **Online Auctions**

B. Internet Banking

C. Online Ticketing

D. Electronic Payments

q. What do you think, after choosing to visit the web store, the consumer is typically connected to_____.

A. **Online transaction server**

B. Private Gateway

C. Processing network

D. Merchants Bank

r. Can you clarify, in which process of e-Commerce, the labelling of product is done.

A. Places an order

B. Order details are entered into your business software

C. Order is passed to the warehouse to be processed

D. **Processing order for Shipping**

s. Can you clarify, which type of E-Commerce focus on consumer dealing with each other.

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. **Consumer-to-Consumer (C2C)**

D. Business-to-Employee (B2E)

t. Can you clarify, Stock availability, item location criteria are mentioned in _____ list.

A. **Pick List**

B. Sample List

C. Product List

D. Payment List

u. What do you think, which of the following basic system functionalities is used to display goods on a Web site?

A. Shopping cart system

B. **Digital Catalog**

C. Customer based database system

D. Product database

v. Can you clarify, which type of E-Commerce deals with auction?

A. B2B

B. C2B

C. B2C

D. **C2C**

w. What do you think, Amazon is a best example of _____ site.

A. Blogging

B. Social Networking

C. **E-commerce**

D. Entertainment

x. What do you think, which of the following is not an example of e-Commerce site?

A. Amazon

B. Flipkart

C. E-bay

D. **Twitter**

y. What do you think, most individuals are familiar with which form of E-commerce.

A. B2B

B. **B2C**

C. C2B

D. C2C

Long Answers

Questions for Remembering

1. What are the different perspectives of E-Commerce?
2. What are the different applications of E-Commerce?
3. Find the benefits of E-Commerce.
4. Identify the Examples of e-Commerce.
5. What are the different architectural models in B2B E-commerce?
6. With a neat diagram Explain how C 2C E-Commerce functions.

Questions for Application

1. Differentiate E-Commerce and Traditional Commerce.
2. Analyse the different phases of E-market with neat diagram.
3. Can you explain the Top-level e-Commerce Process Flow with a neat diagram.
4. Demonstrate the detailed working of receiving orders with neat diagram.
5. Can you explain how the Processing of an Order is done in the Warehouse with neat diagram?

6. Demonstrate the Processing of an Order for Shipping is done explain the concept with neat diagram.

UNIT – II

ELECTRONIC COMMERCE BUSINESS MODELS

2.1 DEFINING A BUSINESS MODEL

A business model is defined as follows:

- A business model describes a set of business entities and interrelationships among them. The model describes the sources of revenue and potential benefits accruing to the involved business participants.
- The business model provides the broad perspective necessary for identifying appropriate solutions at some level of abstraction. The identified solution should be sustainable in terms of revenue and capable of realizing the stated objective.

Electronic commerce has grown at lightning speed due to growth in high speed internet connectivity and evolution in publishing, distribution, payment, and security technologies. To cope with the evolution, business models have been evolving at a meteoric rate. With the emergence of flat fee based internet service providers, online companies had to adjust their business model. With millions of web pages worth of information available on the internet, through flat rate access charges, the metered service became commercially unattractive.

With the increase in the number of web page visitors a newer opportunity emerged. Advertisers discovered a new media, web sites found a new revenue stream. The idea was to build a site with content that would attract a large number of visitors, while simultaneously advertising. In this way these companies would be able to add significantly to the revenue stream. Companies like Yahoo! with over 100 million page views per day and Amazon.com, with 6 million registered users, became an attractive ground for the advertisers. Companies like eBay have popularized the age old auction model and broadened its application by transforming it to a web based auction, transplanted on to the internet.

Some businesses with specialty products found the reach of the internet tempting, which led to the emergence of a new business model, where the producer of specialty products was ready to transact the product for real money, over the internet. Businesses evolved over the internet were content centric in the early days, the later period saw the emergence of transaction focused sites.

2.2 CATEGORIES OF E-COMMERCE BUSINESS MODELS

Over the years, the business models that have emerged on the internet can be broadly classified into four categories:

- Native Content based Models
- Native Transaction Models
- Transplanted Content based Models
- Transplanted Transaction based Models

The taxonomy of the different business models are given in the below figure.

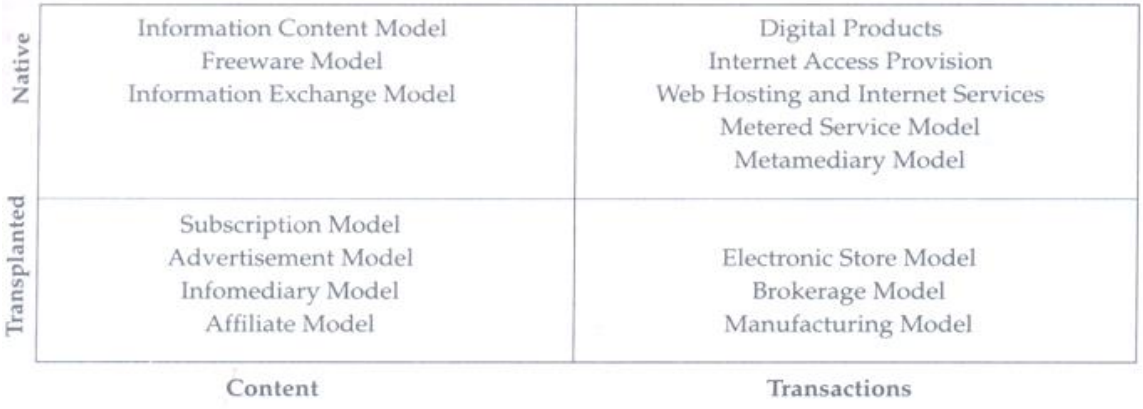


Fig. 2.1 Taxonomy of Internet Commerce Business Models

2.2.1 Native Content Based Models

Native content based models emerged due to the efforts of many amateurs who set up informational web sites expecting no financial returns. Also, a whole lot of software programs and utilities have been available for download-including much of the software that powers the internet-and world wide web which is available free of cost to users from many sites. Based on the nature of content the various models that have appeared include:

1. Information Content Model

The web today is probably the largest source of information, available free of cost to the users. Many websites were set up, containing scientific, country, culture and tourism related information. Attract visitors by offering information in the early stages of Web developments – Major source of Information Contents were scientists, Academicians and Researchers. The Information is typically available at no charge basis. It is typically utilized by agencies and groups interested in wide dissemination of information

For example,

- Virtual Library -- http://www.vlib.org
- International Council of Museums–http://www.icom.org/vlmp
- National Informatics Center, India– http://www.nic.in

2. Freeware Model

This is a model which allows the internet users a free download of internet products and applications. Internet software companies have extensively utilized the freeware model to offer downloads of their products.

- Web browsers by Netscape and Microsoft have been available for free downloads to individual users.
- Linux – http://www.linux.org

- Apache (http://www.apache.org.), is an example of a freeware web service that is popular today, which reaches out to over 50% internet users.
- The **Free Software Foundation** (http://www.gnu.org) develops and maintains archives of UNIX -like operating systems, tools, and utilities available for free distribution over the internet.

3. Information Exchange Model

This model is based upon the exchange of information between individuals and organizations, over the internet. The information captured, during the interaction, about a person can be used for building the profile of individual users. The profile can be later utilized by target marketing and advertising companies for screening out and creating mailing lists. Users may provide information voluntarily as a part of registration process, as is the case with sites like Flipkart.com, Facebook.com and Gmail.com, in order to utilize the services offered by the web site. Users may also provide the information during interaction, in trying to access some information related to the product or service, either directly or indirectly through mechanisms such as Cookies. Many of the news delivery services and targeted advertising services indulge in this model.

2.2.2 Transplanted Content Models

This is a model where companies and other organizations publish the details of their company and related information on their website. With growing acceptability and audience on the internet, many traditional economy businesses saw an opportunity to generate revenues on the internet landscape. The traditional content providers-journals, research databases, directories and advertising-have moved their content to the internet. As a result, information providers and brokers have transplanted businesses on the internet to take advantage of the growing audience.

1. Subscription Model

Content creators and publishers have relied on a subscription based service model. Entertainment and scientific journals, newsmagazines, and other periodic content have been offered, on a subscription basis. Leading publishers and creators of digital content have adapted the subscription based model on the internet. As a consequence, today many journals and magazines are published in digital form as well. In addition many news services and other valuable audio and video content are also available in digital format. The examples of these sites include yahoo.com, udayavani.com, indiatimes.com, etc.

2. Advertising Model

Web sites providing content, e-mail, chat sessions, and discussion forums are utilized for serving advertisements to content viewers. Usually, such sites provide content and services free of cost and generate revenue through the advertisements they display. It is the basis of the growth and success of many search engine companies such as Yahoo! The model is derived

from commercial television and print-publications that make their basic revenue from the advertisement stream. The model has several variations, banner advertisement being the most popular form. **Banner advertisements** are served to millions of users visiting one of these popular sites for content or service. Charges are normally made on the basis of the number of times a banner is served. When the user clicks on the banner he is taken to the web site of sponsor, providing him with more detailed information. The process is called the **click-through** and usually generates additional revenues. The high volume of visitors provide attractive clientele for advertising and promotion. In search engines, it is possible to target banner advertisements based upon search keywords and user profiles leading to higher rates of per million page views. Many specialized portals are based on the advertising model often called vertical portal or **Vortals**, offer a focused group for advertisers in the same vertical segment. For example, Cricinfo (www.cricinfo.com) attracts cricket fans and admirers for gathering news, information and statistics related to cricket and serves as an ideal source for advertising products associated with the game of cricket and outside cricket. Other examples include facebook.com, yahoo.com, msn.com etc.

3. Infomediary Model

An Infomediary company is the one that collects a personal profile from its users (consumers and/or suppliers) and subsequently markets that data to interested set of users, while maintaining the data privacy. In the process it also offers the user a percentage of brokered deals or other services. Consumers incur substantial interaction costs in trying to locate and discover the price of products which changes rapidly due to technological or marketing evolutions. The infomediary model is based on the premise of lowering the interaction cost to consumers during the process of searching for suitable products/services and prices. Businesses based on the infomediary model, address the information demand of consumers by identifying the best deal for them. These new middlemen deliver the value through information mediation rather than the physical distribution. The infomediary model attracts surfers by providing them with useful information about the web sites in a particular market segment that are competing for their money. The infomediary model can also be used to recommend a suitable product to the consumer by matching the customers profile and desired attributes of the product, with the product profiles in its database. For example companies like ePinions (www.epinions.com) facilitate users in exchanging information with each other, about the quality of products and services or purchase experience with merchants.

4. Affiliate model

The affiliate model achieves traffic aggregation for the e-retailer at almost no risk. The affiliate companies offer sales of other manufacturers or e-retailers' (sponsoring merchant's) products on their web sites, for an incentive. The visitors of the affiliate site may choose to click on an item or service offered by the e-retailer at the affiliate web site. The affiliate site redirects the sales transaction to the sponsoring e-retailer or manufacturer, where the actual transaction is carried out. The affiliate sites earn incentive revenue based on the value of each

transaction. Web surfers of various sites, affiliated to the sponsoring web merchant, are aggregated in this model through financial incentives in the form of a percentage of sales value to affiliated partner sites. The affiliates provide a click-through area on their sites to the sponsoring merchant. In the affiliate model the web site generates revenues only if it is able to generate the transaction for the sponsoring site. Thus affiliated sites incur no fixed carrying cost to sponsoring merchants. A very popular example of the affiliate model is Amazon.com.

2.2.3 Native Transaction Models

These are the models that are native to the internet and were either born out of necessity on the Internet or are suited for the IT. These models include-digital product merchandising, internet access provision, providing software and services for creating and maintaining web sites, and finally, a new kind of intermediary that aggregates and presents the information to meet the users objectives rather than those industry segments.

1. Digital Products Merchant Model

The World Wide Web is particularly suited for merchandising digital products as these products can be described, experienced, as well as delivered over the internet. The music, video recordings, pictures, software products, books, documents and data bases are good examples of the products that are available or can be easily transformed into digital form. In this model, also known as the online transaction and delivery model, vendors of digital products or services offer their goods through a web site on the internet. Interested buyers of these goods and/ or services visit the site to obtain information about the products. The product information in a digital goods market may include samples, trial versions and demos, in addition to the usual product attributes and pricing. The buyer matches the acquired information with personal requirements and, if an adequate match is found, may decide to buy the product by clicking on to "buy now" button.

The buyer may select any of the valid online payment mechanisms supported and accepted by the merchant site, such as cyber cash, Master or Visa card, or other electronic payment modes, and provide the required payment related information. The seller, after validating the payment, information and confirming assured payment, initiates the electronic (on-the-wire) delivery of the digital product. Online delivery usually happens by downloading the digital product on the buyer's computer. In the case of services, it may offer the buyer access codes to obtain the service. Examples of these sites include Softwarebuys.com, Brothersoft.com, etc.

2. Internet Access Provision

The basic foundation of electronic commerce rests on the network infrastructure and its growth depends upon the growth in the number of people with access to the Internet. In this model, various companies like America Online, VSNL, MTNL, and Satyam in India, have grown by offering dial-up access to the network. In the dial-up model the ISP business sets up a server in the local calling area of its user base and invites users to sign up for an account with

the company-either as a flat rate or on rates based on duration of usage. Users willing to access the internet dial the phone numbers provided by the ISP and log on with the assigned user id and password. ISP servers are connected to the backbone of the internet. Larger ISPs may have servers in several cities with a local number or even may have the interconnectivity through its own or leased infrastructure. ISPs may offer leased circuits that are dedicated fiber optic connections for faster and relatively assured speed of access. Other alternatives to the traditional access mechanisms, that promise faster access and higher bandwidths, include the cable model and Digital Subscriber Loop (DSL) access. In India Dishnet DSL (www.ddsl.com) is a prime internet service provider with about 10% of the market share.

3. Web Hosting and Internet Services

Many web-based enterprises, including some ISPs and software services companies, provide electronic commerce business infrastructure and support services. These services may include hosting the web pages of the e-businesses and providing them with 24 x 7 availability and services on the internet. In some cases the entire business operation, starting from web page hosting to transaction processing and payment processing is supported by a third party company that specializes and bases its entire business on the model of providing hassle free guaranteed electronic business infrastructure. Several companies such as Yahoo Shops and Lemonade Stand are based on this model. Domain name registration service, electronic mail management services, and search and directory engine registration services are some of the other important service areas that have emerged due to the migration and proliferation of electronic commerce. For example, Pugmarks (www.pugmarks.net) and Verio (WWW.Verio.com) provide web hosting services. Register.com offers domain name registration services and usa.net provides the e-mail management services.

4. Metered Service Model

Software licenses, storage and some computing resources may be required sparingly by organizations sometimes, but they do have to acquire and manage them. Thus it may offload all such responsibilities to a third party company with an adequate degree of resources. The metered service model is built upon providing such an infrastructure to needy companies, based on their rate of utilization. Similarly, the knowledge-resource rich companies can employ the metered service model to charge the knowledge-resource consuming companies based on demand and usage. For example, HP offers Infrastructure on Tap. In this model, customers pay a monthly fee for the use of off-site servers, storage, software, and services. In this model the savings will accrue to the customers because it is HP who owns and manages the infrastructure, maintaining security, ensuring always-on service, scalability during peak periods and handling of upgrades. Thus, customers do not have to worry about retaining the knowledge workers, obsolescence of hardware and software, data security, protection and backup, as well as the round-the-clock availability. One of the most popular and common metered service models is cloud computing where you can store your personal data and files in a cloud server stored at a remote site by paying a certain amount. Some of the premium file download sites also use the

metered service model where the user has to register to the site by paying some money through credit card or other e-payment methods and then he is allowed to download files using the site's server for a particular duration (1 month, 3 months, etc).

5. Metamediaries

A new breed of internet intermediaries who provide information mediation as well as transaction support are called metamediaries. Metamediaries present the information from the users' viewpoint rather than that of the industry segments. With the information being organized by the industry, making multiple transactions for multiple products at multiple business sites inconveniences the users. The metamediary connects customers with providers of related goods and services that fill this need by offering them a virtual trading space called the metamarket, where not only can they acquire all the information but also execute transaction. The revenue model consists of charging a fee on all the transactions that occur of a metamediary's site. In the electronic market, the metamediary establishes itself as a third party web site that horizontally integrates industry segments and provides additional services such as payment settlement, fulfillment, delivery integration, credit offerings and verifications

The role of the metamediary is to provide a multi-vendor catalog that combines product information from various vendors under a single site, providing buyers with a one-stop shopping experience. It may provide further value addition by including information on multiple dimensions of product comparison and product details like quality, inventory availability, as well as the guaranteed delivery dates. The metamediary may adopt the auction model, for transacting unique products with unknown pricing. The metamediary may also work as a forum that serves as an exchange for both buyers and sellers.

2.2.4 Transplanted Transaction Models

Storeowners, catalog-based sellers, manufacturers and brokers-financial, service insurance agents, travel services agents-adapted the traditional business model to increase their reach and reduce the market friction. Three of these models are described here.

1. Electronic Store Model

Catalog based merchandising and mail order companies had a great presence in branded merchandise like audio and video systems and photo cameras, where customers were sure of the nature and quality of the product they were going to receive once they placed a mail/ phone order. The technological foundation of electronic commerce facilitated the task and was readily adopted by catalog-based sellers, and phone/mail order companies as they constructed the web based order business as an additional and more efficient channel. In the web based order business, customers have flexibility to browse and assimilate information and even place a customized order at any hour, without waiting for a sales representative to come online. In this model, customers interact with the seller through a web based interface for gathering and analyzing the information needed for an informed decision. Once the decision about buying a

product has been made, the customer presses the "buy now" button to initiate the purchase process and the seller requests the buyer to select the payment mode acceptable to him. On receiving the payment information, the seller may validate it using payment gateways or the electronic currency provider, as the case may be. Finally, the seller initiates the delivery process by alerting the shipping and handling department to fulfill the order. The shipping and handling of transaction may also be integrated with delivery partners so that pick-ups can be scheduled from appropriate locations for timely delivery. Amazon.com is an example for this model, which started out selling books through web based stores over the internet, at deep discounts compared to traditional brick and mortar bookstore.

2. Brokerage Model

The market makers, also known as brokers, play an important role of facilitating transactions by bringing buyers and sellers together in traditional commerce. The brokers charge a fee or a commission on transactions that are facilitated by them. The brokerage model of traditional commerce has also been adopted in the electronic commerce and has been applied in all the types of e-commerce. In the traditional economy, the brokerage functionality has been pervasive in stock trading, commodity exchange markets, auction markets and multi-level market distributions. The stock market operates through agents, who take orders for buying and selling on behalf of their customers and place them on the stock exchange for matching and fulfilling requests. The process based on phone, fax, and paper has a certain degree of market inefficiency and friction related to the information flow, resulting in a higher transaction commission charged by brokers. The financial brokerage firms like eTrade have grown by going online, incurring lower business costs that in turn result in lower transaction commissions charged to customers by placing the buy or sell order in financial instruments. In general, in the exchange model, brokers earn revenue by charging the seller a transaction fee based on the value of the sale. The auction model can be utilized by businesses to sell excess inventory to consumers or by consumers to sell it to other consumers. The electronic auction provides an internet-based mechanism and generates revenue by usually charging a fee or commission from sellers. BaZee.com, AuctionIndia.com, eBay.com and OLX.in are examples of some good businesses based on this model.

3. Manufacturer Model

In a typical distribution system from the time products are manufactured to the time they reach consumers, it passes through several layers of intermediaries, such as the whole distributor, and local store. Each layer adds to the market friction, thus adding to cost the consumer pays and reducing the profit margin that the manufacturer may get. The manufacturer model is similar to the electronic store model, except here the seller happens to be the manufacturer himself. The manufacturer as a direct seller to the customer through the web offers numerous advantages in the area of customer support and service, product marketing and fulfillment of guarantees. Manufacturers have a better sense of customers' requirements, viewpoints, suggestions, and complaints with regards to the existing products, leading to

improved product offerings and newer products. Dell Computers is an example for this model which started out as a direct seller through the phone order mechanism and transformed itself to harness the powers and advantages offered by the web.

INFORMATION DISTRIBUTION & MESSAGING IN E-COMMERCE

3.1 FTP APPLICATION

FTP or **F**ile **T**ransfer **P**rotocol is the protocol used for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e. g., uploading a Web page file to a server). FTP is used to transfer data from one computer to another over the Internet, or through a network. Specifically, FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet).

There are two computers involved in an FTP transfer: a FTP server and a FTP client. The FTP server, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on.

To transfer a file from the server machine to the client's machine (download), or transfer a file from client's machine to server's machine (upload a file). The FTP supports both batch as well as interactive uses. The protocol only specifies the mode of interaction between the FTP server and clients running on two computers; the user interface is left completely to the client designer.

There are various user The FTP client can browse through the list of files and directories available under the login account. It can request interfaces, ranging from the command line interface to window versions. The typical command line version of the interface can be invoked by typing the command FTP at the prompt. The FTP client responds by requesting the login information. The FTP client reads the commands, types at the prompt, prepares a FTP packet and writes it to the FTP server running at a well-known port of the connected machine. The server prepares a response protocol packet and sends it to the client.

The file transfer application operates through two connections, as control connection needs to be established prior to attempting any file transfers. On making the control connection the FTP server requests authorization information in the form of a user name and password. The authorization information determines whether the files can be accessed by the FTP user. Subject to access permissions, users can transfer files in either direction through "Get" or "Put" command. The files transfer application opens a new connection for the data transfer.

The FTP Architecture is shown in fig. 5.1

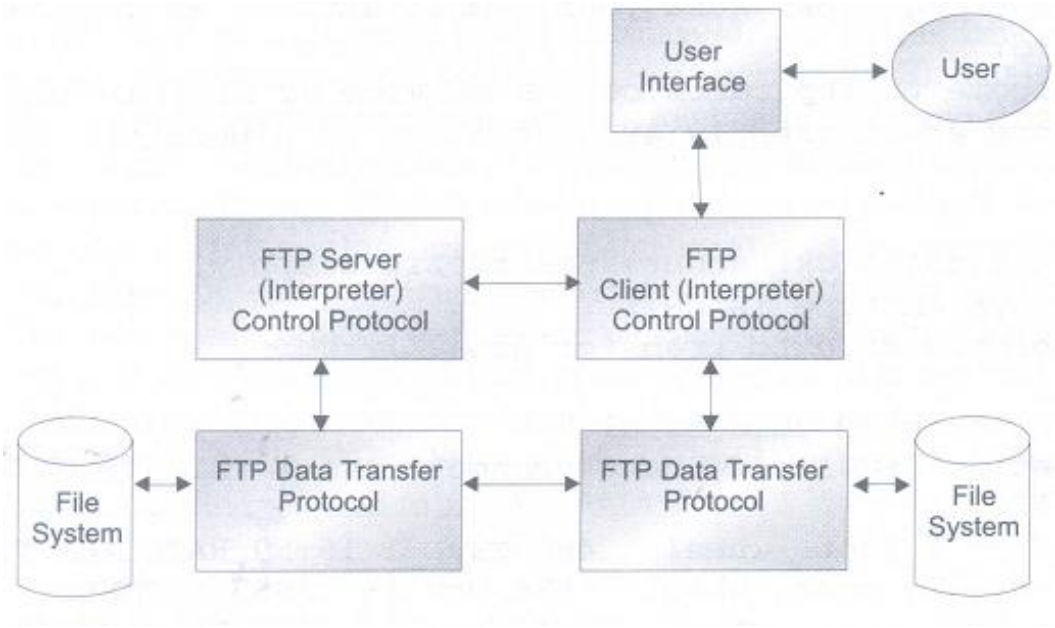


Fig 5.1 File Transfer Architecture

3.2 ELECTRONIC MAIL (E-MAIL)

Electronic mail or Email is the transmission of messages over communications networks. An e-mail system is concerned with the ability to compose messages, move messages from the originator's site to the recipient's site, and report the delivery status to originators, browse messages by the recipients and finally the dispose off the messages. Most e-mail systems include a rudimentary text editor for composing messages, but many allow you to edit your messages using any editor you want. You then send the message to the recipient by specifying the recipient's address. You can also send the same message to several users at once. This is called ***broadcasting***. Sent messages are stored in electronic mailboxes until the recipient fetches them. To see if you have any mail, you may have to check your electronic mailbox periodically, although many systems alert you when mail is received. A typical architecture of the e-mail system (Fig. 5.2) consists of two components to accomplish the functionality- **a user interface program and the message transfer server**.

The user interface, also often called mail reader, is a program that offers users an interface to compose a new message, read a message, reply to senders and delete or file the message. The user interface program (mail reader) provides three functions, i.e. composing, browsing, and disposition. There are a variety of mail readers available. They are built on a character based interface, i.e. a Graphical User Interface (GUI) which is menu and icon driven and accepts inputs from the mouse and keyboard. **Message Transfer Agent (MTA)** programs accomplish the function of transferring the message to the destination. These programs communicate with each other using a standard protocol. A user agent composes a message which contains the destination mailbox address. The message transfer agent connects to the other message transfer agent running on the machine specified in the destination address of the composed message and delivers it through the standard message transfer protocol. In the

internet environment the Simple Message Transfer Protocol (SMTP) has been widely adopted and message transfer agents using the protocol are often referred to as SMTP servers.

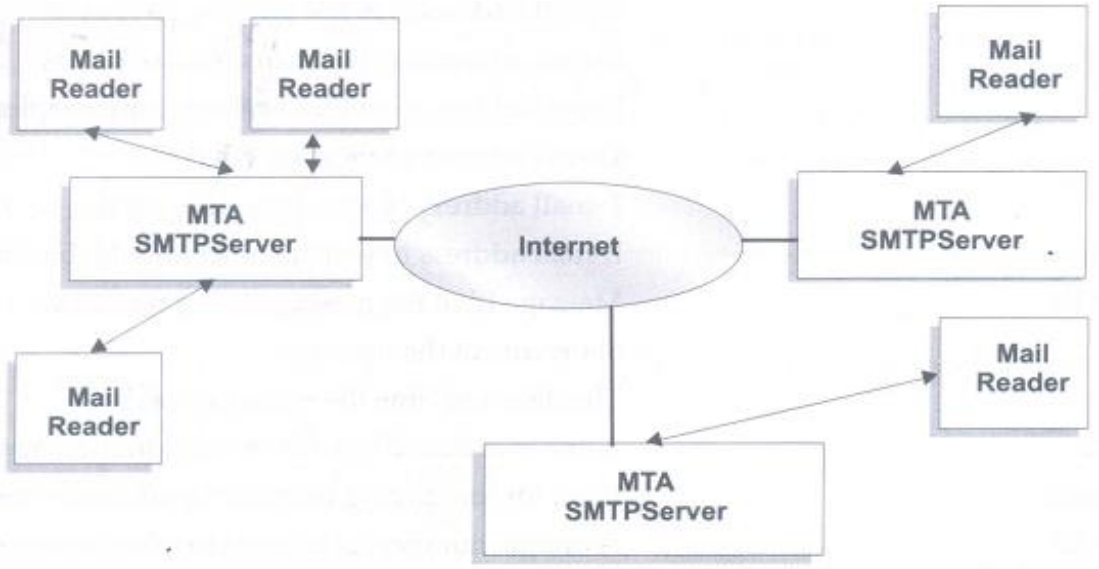


Fig 3.2 Architecture of the E-mail System

As stated earlier, the composed message is communicated to the MTA, which in turn is responsible for transferring it to the destination. The transfer agent uses the information contained in the message to find out the address of the machine and mailbox id (or username) for the final delivery. In the internet environment the message, handed over by the user agent to the message transfer agent, follows a standard format described in RFC 822 and servers using SMTP accomplish the message transfer.

Message Format

The format of an e-mail message, composed by the user agent, is described in RFC-822, available on the internet. The original RFC 822 format was designed for handling text only mails, but later was enhanced to use multimedia extensions, by supplementing the header fields. The message consists of standard lines of text messages in the "memo' format. As in a memo, it has a header portion that follows a rigid specification and the body of the message portion that is a free flowing text. The header portion consists of two types of field-the rigidly formatted, and the user defined. Some of the rigidly formatted fields contain information regarding the message transport and delivery and are used by message transfer agents, while the rest of them are used by the user agents or recipients. Some of the fields used in RFC 822 message format are shown in Table 3.3.

Header Field Name	**Description**
To	E-mail addresses of primary recipients

From	E-mail addresses of message creator
CC	E-mail addresses of carbon copy recipients' E-mail addresses
BCC	Blind of carbon copy recipients
Sender	E-mail addresses of actual message sender
Reply To	E-mail addresses to which reply should be sent
Subject	Short Title of the message
Date	The date and time message was sent
Return path	Identifies the return path to the sender
Message Id	A unique identifier for referencing this message later

Message Transfer

Message transfer agents (MTA) are responsible for delivering the message to the destination machine. In the Internet environment, the SMTP is widely used by message transfer agents. Simple Mail Transfer Protocol (SMTP) is an ASCII based protocol. In a typical message transfer between two SMTP daemons, the sender makes a TCP based connection to the daemon running at port 23 of the machine specified in address field of the header. On successful establishment of connection, the message is transferred to the destination daemon using SMTP. The message transfer follows the envelope and content model. The envelope is constructed from the "From:" and "To:" fields of message format. In a typical session between two SMTP daemons, the receiving daemon accepting a connection request from the sender responds by sending a welcome message. For example the sender daemon responds with the 'HELLO' command and informs it about its own domain. After the handshake phase, the address on the envelope is used by the sender daemon to establish the data transfer to the right user on the receiving side. The sender daemon communicates, to the receiver, the protocol packet containing a 'From' address followed by the recipients' addresses one at a time. The receiving daemon responds each of the protocol packets, either with an "Okay", or with a specific error message.

One generic application that offers information / file management and delivery services is called **Mail Server**. A mail server accepts all the incoming messages destined for a specific userid processes the body of message as a list of commands. Typically, the subject line is blank and the mail server ignores it. The mail server running at the machine sends back the files available at the site locating a useful file, the user may send another mail with the message body containing 'file <filename>' and will receive the file by e-mail.

3.3 WORLD WIDE WEB SERVER (WWW SERVER)

The concept of the World Wide Web (WWW) was born, out of an experimental system developed at CERN (European Laboratory of Particle Physics) with the objective of enabling document sharing among scientists, in 1989. A prototype system offering the ability to inter link multimedia documents, distributed over the network through the concept of hyperlinks, was developed at CERN. The developed system offered an intuitive and logical interface that makes it easier to browse textual, graphical, audio and video information integrated on the same screen.

The original architecture proposed by Tim Berner Lee consisted of documents stored and managed on server machines and client processes, running on distant or even the same machine. The server software was envisaged to be a process that receives requests from the client processes and replies to them by delivering appropriate documents. In the proposed system the client and server processes run on machines connected on the same network. The architecture consisted of two building blocks - the server and the client processes, communicating on the same network.

The World Wide Web became extremely popular as the client programs or browsers available offered an easy to use graphical user interface and the ability to point and click in order to access any hyper-linked information. The server accepts browser requests and manages the delivery of documents to the browser. The documents contain hyper-links, rich text and multimedia information.

The World Wide Web is the combination of four basic ideas:

- **Hypertext**: A format of information which allows, in a computer environment, one to move from one part of a document to another or from one document to another through internal connections among these documents (called "hyperlinks").
- **Resource Identifiers**: Unique identifiers used to locate a particular resource (computer file, document or other resource) on the network - this is commonly known as a URL. In the World Wide Web, unique **Uniform Resource Locator (URL)** defines each published document. A URL consists of the three components. The first component, prefixed and separated by / /, describes the protocol server; for the web it is 'http'. The second component, the text starting after / / and ending with the' /' or end of string, describes the domain name of the server, for example www.google.com. The third component, beginning with the / and finishing with the end of string or ':', describes the document name at the server. The web server waits for client connections and requests at the port 80, as a standard convention.

  Examples of a URL: http://www.w3shools.com

  http://www.w3schools.com/index.html

  http://www.w3schools.com/index.html:8080

- **Markup language**: Characters Codes embedded in text which indicates structure, semantic meaning, or advice on presentation. The Hypertext Markup Language **HTML** is used for constructing these documents. An HTML file is a text file

containing small markup tags which tells the Web browser how to display the webpage on the internet. The request-reply paradigm between the browser and the server follows a standard protocol, called **HyperText Transfer Protocol (HTTP)**.

- **The Client-server model of computing**: A system in which client software or a client computer makes requests of server software or a server computer that provides the client with resources or services, such as data or files

In normal operation, a user types the URL on the address bar of the browser. The browser parses the URL to determine the domain name, document name and the port number at which to contact the server. The browser contacts the servers and uses HTTP to retrieve the specified document from the server. The retrieved HTML document is then parsed and rendered on the screen by the browser. The interaction between the browser and web servers take place in the format described in HTTP.

3.4 HYPERTEXT TRANSFER PROTOCOL (HTTP)

Hypertext Transfer protocol is set of rules that World Wide Web clients and servers use to communicate over the network. It is a connectionless protocol, meaning that browsers and servers do not establish a permanent connection. A client opens a connection and submits a request message to a server. The server on receiving a message processes and responds to it and closes the connection. It is also a stateless protocol, implying that the server does not maintain any information on the state of the process. Thus, the server treats each request/message independent of any previous requests/messages. The protocol is based on the request/response model.

The client, usually a web browser, submits a request to a web server. The server reads the incoming protocol packet, processes it and sends the response. The content type is built as part of the protocol's response packet. The browser has to be aware of the type of multimedia content delivered to it as a response. The content types used in the protocol are a subset of the standard MIME types. The browser connects to the server machine, specified by domain name/IP address, at the specified or standard port. On making a successful connection, the browser submits an HTTP request. A typical HTTP session between the client and server is depicted in Fig. 3.4. The session consists of two phases: the first phase consists of the client's request submission, while the second phase consists of the server’s response. The client submission, depicted in three steps, involves opening a connection, sending the request and header information.

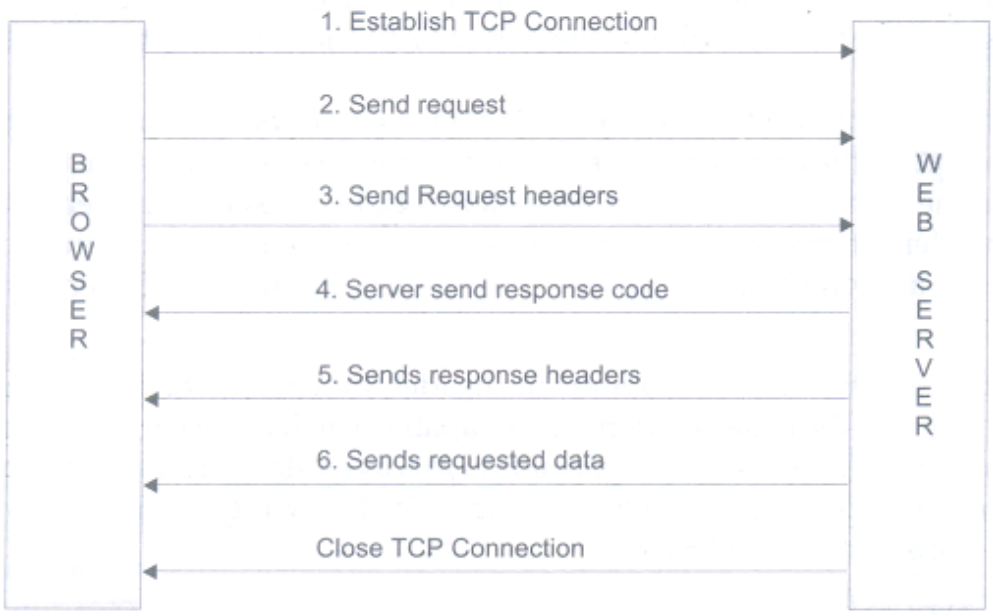


Fig 3.4 Typical interaction in an HTTP session

Following are the steps that take place in a typical interaction of an HTTP session

- **Step 1**: HTTP packets can be transmitted only after the client has established a connection with the server. In this step the browser parses the URL for identifying the domain name. It uses the services of Domain Name Server (DNS) to resolve the name into an IP address. Using the services offered by the TCP layer, it opens a connection to the IP address, at a standard web or URL specified port. On the successful opening of a connection, the browser starts the HTTP session.

- **Step 2**: The browser submits HTTP packets containing the request command to the connected server. The common HTTP request commands are "get", "post", and "head". The request in HTTP is made up of three components: the command method, resource identifier and the protocol version number. An example of the "GET" command is as follows:

  GET /index.html http/l.0

  The method describes the type of request and determines the response at the server end. The second component is a resource identifier, such as the name of a file to be retrieved. Parsing the URL and stripping out the protocol name, domain name, and port number (if present), derives the resource identifier from the URL. The last component of the request specifies the version number of protocol being used.

  In case of an interactive session, that uses forms for submitting the data to be processed by the common gateway interface (CGI) mechanism of the HTTP server, the request line also contains data as a part of the resource identifier (URL). The 'post method' is devised as an alternative mechanism for submitting the form data entered at the browser end, to the server for processing. Unlike the' get method' that appends the form data to

the URL, the post method sends the data as a part of the header information along with the data.

- **Step 3**: In this step the browser submits the header information to the server. The header information includes the browser identity, its capability to handle various types of content and the referring URL. The header information follows a standard format of header name and the value pair, separated by the colon (:) sign. The header information is read and processed by the server and is made available at the server end as environment variables. In case of the 'post method' the browser as part of the header information also submits the form-data, content-type and content-length.

- **Step 4**: On receiving the client request and header information, the server processes the request and sends the response to the client. If the request was processed and can be delivered, the server sends an OK response. Some common errors that it may send as responses include forbidden document, 'not found', 'internal server error', 'or' 'unauthorized access'. The format of the response sent by the server includes the protocol version followed by the response code. The protocol version informs the client about the kind of syntax used in responses. Examples of server responses are as follows:

  HTTP/1.0 200 OK

  HTTP/1.0 404 Not Found

  HTTP/1.0 401 Unauthorized

  HTTP/1.0 403 Forbidden

  The clients use the code part for interpreting the response and acting accordingly. The message part is displayed to users. For example on receiving the response code of "200 OK" the browser understands that the request was processed successfully and proceeds to receive the data that it had requested.

- **Step 5**: Prior to sending the requested data, the server sends information about the data, such as the type of content and length of content as well as information about the server itself, as part of the response phase. The response headers sent by servers are also used at times, for accomplishing authentication and setting up cookies. The response header information follows the same syntax as request headers. The following example shows typical response header information.

  Date: Tue, 04 Sept 2001, 10:40:05 GMT

  Server: Apache/2.1.2

  Last-Modified: Sun, 02 Sept 2001, 08:05:10 GMT

  Content-Length: 8455

  Content-Type: text/html

  The above header information informs the browser of the date and time at which the server response was sent and the name and version of the server software. It also informs the browser of document-related information. The Last-Modified date tells the

user when the requested document was last updated. The last two headers tell the browser about the length of the requested documents, in bytes and the type of content.

- **Step 6**: The server, after sending the last response header information, sends a blank line to indicate the completion of header portion the response and to mark the beginning of the response data. The server sends the response data to the browser in the format indicated in the content-type response header.

- **Step 7**: The web server, on completing the data transmission, is done with responding to the client request. At this stage, it would ordinarily close the TCP connection. However, an HTML document may contain online images and embedded objects required for rendering it on the browser screen. Although the browser can submit a request for retrieving each of these objects, by opening a new connection to the same as follows:

  Connection: keep-alive

  In this case the server keeps the TCP connection open even after the response data has been sent. The browser uses the same connection for the subsequent request.

3.5 WEB SERVERS IMPLEMENTATION

There are several implementations of web servers on the internet. The original implementation done by Tim Berner-Lee's team came to be known as the **CERN** implementation. The CERN implementation of web server (CERN httpd) was maintained and supported for full features up till 1996. The CERN version has also been known as the **World Wide Web Consortium (W3C) httpd**. With the release of the Jigsaw web server by W3C the CERN httpd is no longer supported. The W3C Jigsaw web server is also a public domain, open source project of W3C. It supports the full version of HTTP 1.1, with advance features, and is implemented in JAVA unlike the CERN httpd that was implemented in C and supported HTTP 1.0 protocol.

The other public domain implementation was by Rob McCool's team at the National Center for Supercomputing Applications (NCSA) and was widely deployed in a short period of time. The server was a public domain, open source software and was supported and enhanced up till 1994 at the NCSA. Most commercial implementations of web servers have been based on one of these two architectures. The Netscape web server is based on the NCSA httpd architecture.

Using the NCSA httpd version 1.3 as the code base, all known bug fixes and enhancements were incorporated by the core team and it was released as the Apache version 0.6.2, around April 1995. Then the Apache version 1.0 based on the new architecture was released in December 1995. The Apache development is managed by group of volunteers, around the world, connected through the internet. The team uses the internet and the web for communicating, planning, developing, bug-fixing, reporting and documenting the web server.

Today, web servers provide the following four major functions.

- Serving static web pages

- Serving web pages generated by running gateway programs
- Controlling access to the server
- Logging server access and error statistics

NCSA Web Server

The NCSA web was the most deployed server till the emergence of the Apache server, based upon the NCSA HTTPD version 1.3. The NCSA server was ported and made available on a variety of UNIX versions including Linux, Irix, IBM AIX, Solaris, SunOS, Ultrix, etc. In the location of the installed files is guided by the value of environment variable "**Server root**". The Server Root Directory Contains conf, logs, cgi-bin, and support sub directories. On startup the HTTPD looks for the file conf/httpd.conf in the Server Root directory. The **'cgi-bin'** directory stores executable binary **sHipts** that can be executed from the HTTPD server. The **'htdocs'** directory holds the starting document, i.e., home page and other related documents. The 'logs' directory maintains server logs showing access requests and errors. The 'conf' directory stores the main configuration files for the server and customizes the server through the three configuration files, viz. **httpd.conf, access.conf** and **srm.conf**.

The HTTPD server configuration file 'httpd.conf' controls the server configuration through a slew of directives. The configurable parameters include the IP address, port number, number of children the server will launch at one time, maximum number of children processes it will have at any time. Log files are stored in the logs directory as per the name specified in the httpd.conf. The server is capable of logging document transfer, errors, accessing agents and referrers related information. The access.conf file manages the access control. The file contains directives to control access for setting up controls over the types of requests and transfers. It can also set up user / password based authentication on the server. The third configuration file maintains the server resource map in srm.conf.

Apache Web Server

The Apache software foundation distributes the web server under a public domain software license policy. It can be freely downloaded and installed from the Apache web site (www.apache.org). The latest version of source files for installing the apache web server can be downloaded by browsing the location http://www.apache.org/dist/httpd/httpd -2 0 NN.tar.gz Files can be extracted, compiled, and configured through the 'makefile' provided as a part of the download.

Apache supports a variety of operating system platforms, including versions of Unix, such as AIX, BS200-0SD, Dgux, Digitalunix, Freebsd, Hpux, Irix, Linux, Netbsd, Netware, Openbsd, Osf/l, Solaris, and Sunos. Apache web server binaries are also available for Macosx, Macosxserver, Os/2, and Win32 environments.

Once the binary version has been compiled and created or downloaded, the installation process requires customizing configuration files for the server. The Apache server configuration directives reside in three main configuration files. The installation process sets

up the environment to run the httpd from the default directory defined by the Server Root. The configuration files are located in the conf sub directory and are called srm.conf, access.conf and httpd.conf. The conf directory also contains sample configuration files named srm.conf-dist, access.conf-dist and httpd.conf-dist. These files can be copied and and edited to provide custom values for the directives. Inappropriate or erroneous setting of values for directives may lead to misconfiguration of the server or may even cause the server not to function, or still worse may lead to security gaps.

MULTIPLE CHOICE QUESTIONS

Questions for Understanding

a. Can you clarify which of the following describes a set of business entities and interrelationships among them?
   - **A. Business Model**
   - B. Account Model
   - C. Transaction Model
   - D. Inventory Model

b. What do you think, _____ provides the broad perspective necessary for identifying appropriate solutions at some level of abstraction.
   - **A. Business Model**
   - B. Account Model
   - C. Transaction Model
   - D. Inventory Model

c. Can you clarify, which allows the internet users a free download of internet products and applications?
   - A. Business Model
   - B. Account Model
   - C. Transaction Model
   - **D. Freeware Model**

d. What do you think the Full form of FTP is?
   - **A. File Transfer Protocol**
   - B. File Transfer Program
   - C. Fund Transfer Protocol
   - D. Fund Transfer Program

e. What do you think the Full Form of MTA is?
   - A. **Message Transfer Agent**
   - B. Message Transfer Aid
   - C. Media Transfer Agent
   - D. Media Timed Agent

f. Can you clarify, which field of Email has Blind of carbon copy recipients in it.
   - A. To
   - B. From

C. CC
D. **BCC**

g. Can you clarify, which field of Email has Short Title of the message?
   A. From
   B. Subject
   C. CC
   D. BCC

h. What do you think the Full Form of SMTP is?
   A. **Simple Mail Transfer Protocol**
   B. Small Mail Transfer Protocol
   C. Sample Mail Transfer Protocol
   D. Switched Mail Transfer Protocol

i. What do you think the Full form of CGI is?
   A. Common gateway interface
   B. Client gateway interface
   C. Client gap interface
   D. Common gap interface

j. Can you clarify, Server Response with value HTTP/1.0 200 means what?
   A. OK
   B. Not Found
   C. Unauthorized
   D. Forbidden

k. Can you clarify, Server Response with value HTTP/1.0 401 means what?
   A. OK
   B. Not Found
   C. **Unauthorized**
   D. Forbidden

l. What do you think the Full Form of DNS is?
   A. Domain Name Server
   B. Data New Server
   C. Domain New Server
   D. Data Name Sever

m. Can you clarify, which field of Email has Short Title of the message?

A. From
B. Subject
C. CC
D. BCC

Questions for Skill

n. Do you know _____ describes the sources of revenue and potential benefits accruing to the involved business participants?
A. Business Model
B. Account Model
C. Transaction Model
D. Inventory Model

o. Do you know _____ is the oldest catalogue of the web which is run by a loose confederation of volunteers?
A. Traditional Library
B. Virtual Library
C. Physical Library
D. Book

p. Do you know, _____ is based upon the exchange of information between individuals and organizations, over the internet?
A. Business Exchange Model
B. Traditional Exchange Model
C. Information Exchange Model
D. Discounted Exchange Model

q. Do you know, _____where companies and other organizations publish the details of their company and related information on their website?
A. Native Content Model
B. Native Transaction Model
C. Transplanted Content Model
D. Transplanted Transaction Model

r. Do you know, _____ is the one that collects a personal profile from its users and subsequently markets that data to interested set of users, while maintaining the data privacy?
A. Infomediary Model
B. Metamediaries Model
C. Data Model

D. Business Model

s. Which of the following achieves traffic aggregation for the e-retailer at almost no risk?
   A. Infomediary Model
   B. Metamediaries Model
   C. Affiliate Model
   D. Business Model

t. Do you know, a new breed of internet intermediaries who provide information mediation as well as transaction support are called _____.
   A. Infomediary
   B. Metamediaries
   C. Data
   D. Business

u. How many categories are present in Transplanted Transaction Models?
   A. 2
   B. 3
   C. 4
   D. 5

v. How many categories of Business models exist?
   A. 2
   B. 3
   C. 4
   D. 5

w. Do you know, sending the same message to several users at once is called as?
   A. Serial Transmission
   B. Broadcasting
   C. Parallel Transmission
   D. Unicasting

x. Do you know, a format of information which allows, in a computer environment, one to move from one part of a document to another or from one document to another through internal connections among these documents is called as?
   A. Hyperlink
   B. Linker
   C. Loader
   D. Connector

y. Do you know, the header information follows a standard format of header name and the value pair, separated by which sign.

A. :

B. ;

C. .

D. ,

Long Answers

Questions for Understanding

1. Explain native content based model.
2. Explain a transplanted content model.
3. Explain Digital Products Merchant Model
4. Illustrate Metamediaries model
5. Explain transplanted transaction model.
6. Illustrate e-mail concept
7. Can you explain the combination of four basic ideas in World Wide Web?
8. Illustrate the fields used in RFC 822 message format
9. Write in your own words about FTP
10. Write a note on Apache Web Server.
11. Illustrate the steps in a typical interaction of an HTTP session with a neat diagram
12. What is a business model? Mention different categories of e-commerce business models with taxonomy diagram.

UNIT – III

ELECTRONIC DATA INTERCHANGE

4.1 CONVENTIONAL TRADING PROCESS

A typical trading process defines the relationship between a manufacturing organization and a consumer organization. A conventional trading process consists of the following steps:

1. Either the inventory management system-based on a re-order policy following the examination of the stock levels-raises the purchase requisition for the item or a department raises the requirement for some items. The information on the requisition forms is entered into the purchase processing system. Many a time there are transcription errors in the process. Thus, it is necessary to edit and correct the data.
2. Once the correct requisition information has been updated in the computerized purchase system, the purchase management system scans the suppliers' databases for potential suppliers and prints the purchase requisitions (PRs), requesting the price and delivery quotation in the name of screened suppliers.
3. The purchase requests are transmitted to the suppliers, either through phone/fax or through mail / courier service.
4. The information printed on the purchase requests may be keyed in by the suppliers in their computerized systems for processing, and a quotation against the purchase request may be prepared and printed.
5. The quotation from the supplier is transmitted using traditional paper transmission mechanisms such as fax/ courier / mail service.
6. All quotations, received from suppliers against a purchase request, are entered into the manufacturer's automated system and edited and corrected to remove any transcription errors.
7. The order is then printed on a standardized order form along with the terms and conditions for delivery and payment.
8. The printed order is mailed, couriered, or faxed to the supplier.
9. The supplier, on receiving the order, enters it into the computer system and matches the order with the quotation that has been submitted.
10. If everything is found in order, it raises an internal sales order which requires data entry/editing of the information from the received purchase order, matching and processing of the order, and then printing of the internal sales order.
11. The appropriate stock is thus picked and packed for sending it to the buyer along with the packing list and advance shipping note and advice. The process, at times, may lead to a partial fulfilment of the order. In that case, the customer needs to be informed of the short-delivery and order-status in writing.
12. With the goods, the internal sales-order processing system also prepares a delivery note which is sent to the buyer using postal mail/ courier / fax services.
13. The buyer or receiver, on receiving the goods and advices, compares and inspects the goods, and prepares a goods receipt note containing the purchase order number against which the goods are received, and marks the acceptance and rejection of the items

shipped. The information on the goods receipt note is transcribed at the computer department, edited, and matched against the outstanding purchase-order. In case of partial delivery, steps 9-13 are repeated several times until the quantities on the order are fulfilled.

14. The supplier's computer, on completion of the order fulfilment, also generates an invoice by printing it, which, in turn, is dispatched to the buyer/manufacturer.
15. The supplier's computer also generates a financial statement at the end of the trading month for the payments. At times it also keeps sending reminders for the payment till the complete payment have been received from the buyer.
16. The buyer's computer enters the information on the payment (demand) statement, matches it against the purchase order, and also matches it against the information provided by goods receipt note or, in other words, ensures that the order has been fulfilled and has been inspected and accepted. If everything is found to be in order the buyer's computer processes the order payment.

4.2 ELECTRONIC DATA INTERCHANGE (EDI)

EDI is the exchange of business documents between any two trading partners in a structured, machine-readable form. It can be used to electronically transmit documents such as purchase-orders, invoices, shipping bills, receiving advices and other standard business correspondence between trading partners. EDI can also be used in exchanging financial information and payments in electronic form.

The **Electronic Fund Transfer (EFT)** systems used by financial institutions are a prime example of the application of EDI in the banking and financial sector. EFT is defined as any transfer of funds initiated through an electronic terminal, telephonic instrument, or computer to order, instruct or authorize a financial institution to debit or credit an account. It deals with moving funds from one financial institution to another

EDI should not be viewed as simply a way of replacing paper documents and traditional methods of transmission such as mail, phone, or in-person delivery with electronic transmission. Rather, it should be seen as a means to streamline procedures and improve efficiency and productivity. EDI covers wide and varied application areas and, depending upon the perspective, has been defined in several ways.

According to the Data Interchange Standards Association (DISA), "Electronic Data Interchange (EDI) is the computer-to-computer exchange of business data in standard formats. The Webopedia says that, "Electronic data interchange, is the transfer of data between different companies using networks, such as the Internet. According to the EDI University, a training provider in EDI, "EDI stands for Electronic Data Interchange, a method of transporting all types of information, such as purchase orders, invoices, payments and even graphics, to another party electronically.

The National Institute of Standards and Technology says that, "EDI is the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of

whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media."

4.3 BUILDING BLOCKS OF EDI SYSTEM: LAYERED ARCHITECTURE

The two key concepts in an e-commerce system are electronic document exchange and electronic messages that need to be addressed for an EDI system to evolve. The electronic messages/documents that can be interpreted and understood by various purchase and order processing the systems deployed at different vendors are heterogeneous in nature. Thus, evolution of a general purpose EDI system requires addressing of the problem of heterogeneity at two levels-exchanging documents over heterogeneous networks and the heterogeneity of document formats.

The general architecture of the EDI system consists of four layers:

- The Application-conversion layer
- Standard message formats layer
- The Data Transport layer
- The Interconnection layer

The layered architecture of an EDI system is shown in Fig. 3.1

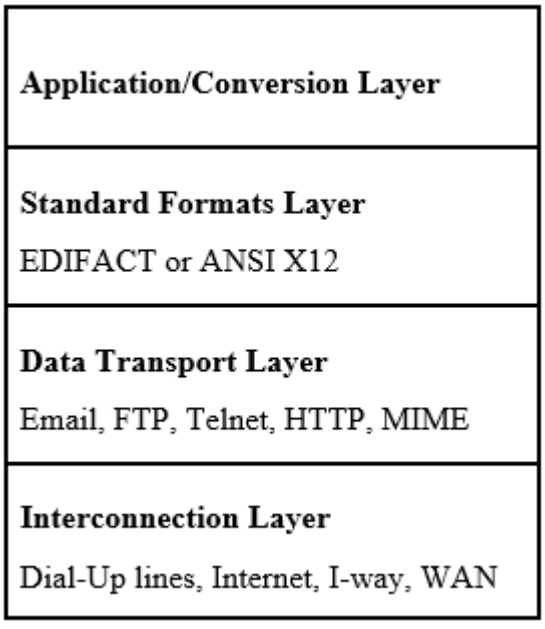


Fig 4.1 Layered architecture of EDI systems

1. Application/Conversion Layer

The application layer consists of the actual business applications that are going to be connected through the EDI systems for exchange of electronic information. These applications

may use their own electronic record formats and document formats for storing, retrieving, and processing the information within each company's systems. Since each company's system may have its own proprietary format, which would be used by their system(s), for EDI to operate, they need to convert the internal company document format to a format that can be understood by the system used by the trading partner. When the trading partners are small in number, converters for various partners' formats can be built. But, as the number of partners with different internal formats increase, the task of building converters for each proprietary format to other formats becomes overwhelming.

The problem of heterogeneity of formats can be better addressed using a common standard format for documents/messages transferred within the EDI system. The internal processing systems continue to use the proprietary formats, but, for transmission over the wire, they adopt a common document/message format. In this case the conversion program learns to translate the common message format to the proprietary message format used by a system, and vice-versa. The approach greatly simplifies the problem posed by heterogeneity of proprietary message formats, as depicted in Fig. 3.2.

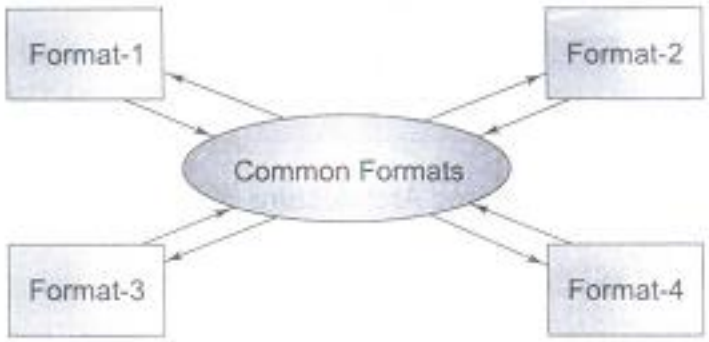


Fig 3.2 Common formats approach in EDI

2. The Standard Formats Layer

The important and critical building block of the EDI system is standards for business documents/forms. Since the sender and receiver in the EDI systems have to exchange business documents that can be interpreted by all parties, it has necessitated the development of form standards in EDI. EDI form standards are basically data standards in that they lay down the syntax and semantics of the data being exchanged. Some of the early and dominant adopters of EDI, like the transport industry in the United States, took the lead in developing these standards. The large retailers also saw the benefits of adopting EDI and went on to develop unique standards suited to their individual requirements. The shipping industry devised a set of standards called Data Interchange for Shipping (DISH), the automobile sector came up with a standard under the umbrella of Organization for Data Exchange by Tele Transmission in Europe (ODETTE). The need for an industry-wide EDI standard was widely felt and this lead to the formation of a Standard Committee X12 under the auspices of American National Standards Institute (ANSI).

Document Standards

The cross-industry standardization of documents is at the core of smooth functioning of EDI systems. The interconnection among trading partners only serves the purposing of exchanging information, but a document exchanged between two trading partners needs to be recognized and interpreted correctly by the corresponding software systems running at various partners' computers. For example, a purchase order needs to be identified by all the EDI applications running on trading partners' computers as being a purchase order from a particular organization. Over a period of time, two major EDI standards have evolved.

The first, commonly known as **X12**, was developed by the Accredited Standards X12committee of the American National Standards Institute (ANSI) and the second, the International standard, was developed by the United Nations known as EDI for Administration, Commerce and Trade (**EDIFACT**).

ANSI X12 Standards

The X12 standard developed by ANSI sets the framework and rules for electronic data interchange. It describes the format for structuring the data, the types of documents that should be transmitted electronically and the content of each document. The identification numbers for various forms, codes for a variety of fields, and types of information is also defined in the standard. The standard also defines the sequence of information flow. The X12 devised the standards to deal with transactions such as purchase order placement, order processing, shipping, invoicing, and payments, to name a few. In the X12 standard, paper documents related to particular business activities are mapped into a transaction set. Each transaction set is given a numeric code and each transaction set is used and for defining the transfer of a single document (purchase order, manifest etc.) between the computers of two trading partners. The X12 document can be thought of as containing three distinct types of information-header, detail, and summary.

EDIFACT -An International Standard

In 1987, the United Nations announced an international standard called EDI for Administration, Commerce, and Transport (EDIFACT). The EDIFACT standard is promoted by the United Nations Economic Commission, which is responsible for the adoption and standardization of messages. The International Standards Organization (ISO) has been entrusted with the responsibility of developing the syntax and data dictionary for EDIFACT. EDIFACT serves the purpose of trans-border standardization of EDI messages. EDIFACT combines the efforts of American National Standards Institute's ASC X12, Trade Data Interchange (TDI) standards developed and deployed by much of Europe and the United Kingdom.

3. Data Transport Layer

In a typical purchase process, once a purchase order has been prepared and printed in the standard format, it is placed in an envelope and dispatched through postal or courier services to the supplier. The content and structure of the purchase order is defined in the standards layer (as described in preceding section) and is separate from the transport/carrier mechanism. The layer utilizes any of the available network transport services such as **Electronic mail (E-mail)**, **File Transfer Protocol (FTP)**, **Telnet** based remote connection and transfer or even the **Hyper Text Transfer Protocol (HTTP)** that drives the World Wide Web. Electronic mail has emerged as the dominant means for transporting EDI messages. EDI documents/messages are exchanged through the network infrastructure as electronic mail messages. Electronic mail is used only as a carrier for transporting formatted EDI messages by the EDI Document Transport Layer. The structured message, delivered by the electronic mail, is interpreted by the receiving software, which is capable of comprehending the structure of the EDI standard information. ITU-T has adopted X.435 (X.400-based) standards to support electronic data interchange (EDI) messaging. Unlike the normal electronic mail message transfers, EDI messages are used for business transactions and security acquires paramount importance. The integrity of the message ensuring that the message has not been tampered with, intentionally or inadvertently, during the transit-and the non-repudiation-ensuring that neither party can deny sending the EDI business form once it has been sent or received-have to be in-built in the transport standards, structure and processes.

4. Interconnection Layer

The interconnection layer refers to the network infrastructure that is used for the exchange of information between trading partners. In the simplest and most basic form it may consist of dial-up lines where trading partners dial-up through modems to each other and connect to exchange messages. In case of the direct dial-up connections, partner computers have to be available for online connectivity and ready to receive the data at all times. Additionally, direct connections between partners have further problems as each partner has to establish a number of direct connections with all the partners.

Leased lines and I-way, Internet or any reliable network infrastructure that can provide interconnection can be used. Through interconnection, EDI partners are able to achieve document exchanges between themselves. The information entered by the trading partner on his/her computer screen, or the document transfer request initiated by some process in the trading partner's computer travels to the receiving partner's computer through the network routes and pathways. EDI messages received on the partner's computer are processed for correctness of format, interpretation, and then inserted for processing into the internal system. The receiving partner's computer has to carry out a variety of tasks, such as identifying the standards, translation from standards to local systems, and then initiating the request/order processing from the local system.

4.4 VALUE ADDED NETWORKS

Value-added network or VAN is a convenient method for conducting EDI which provides functionalities related to connectivity and common services such as continuous presence for receiving and sending documents often implemented through mailboxes, protocol conversion, implementation assistance, security and auditing are handled by the value added network provider.

In other words, Value Added Networks (VANs) are third-party communication networks established for exchanging EDI traffic amongst partners. Various businesses (trading partners) subscribe to VAN services. For every subscriber, the VAN maintains an account, which serves as an electronic post box for the subscriber, for sending and receiving EDI messages. There are a number of third-party value added network providers in the market place. Many VANs today also offer document exchange ability of EDI documents with other VANs. Typically a company subscribes to a VAN to give some network services like EDI translation, encryption, secure e-mail, management reporting and other extra services for their customers.

The typical services provided by value added networks are as follows:

1. Document conversion from one standard to another; typically required when two trading partners use different standards for EDI exchanges, i.e., ANSI ASC X12 to EDIFACT or TDCC to ANSI ASC X12.
2. The sender may follow certain conventions that are different from the receiver. VANs can also provide translation from a sender's conventions of a standard document to the receiver's conventions; i.e.
    - Translate field separators
    - Discard unwanted characters
    - Format translation from edi standard to or from flat file, flat file to flat file, xml and other formats
    - Data translation among the pdf, xls, mdb, or other web- based documents.
3. The appropriate customer data can be saved in the VAN account and later appended on messages where required.
4. The VAN provider's computers also store data such as customer profiles, repetitive waybill codes, etc. which can be used for filling up the EDI transaction document with the help of the customer profile code. The customer profile stored on the VAN can be accessed using the customer profile code and the data from the profile stored on the VAN can be used for completing the EDI transaction.
5. Subscribers can interactively enquire about the status of any EDI transaction made by them.
6. Subscribers can receive "verify acknowledgments" in the mailbox even when they are not online.
7. The VAN can alert the subscriber (receiver) that there is data in their mailbox to be picked up:
    - By sending a fax notification

- By calling a pager or other alerting devices that signal users about the waiting mail in the mailbox.

8. The VAN can capture the specified data from transactions which, in turn, can be used for generating customer-specified reports.
9. The subscriber may specify the editing requirements, which can be edited by the VAN for completeness and correctness, as per requirements. For example, it can verify that the line item charges on an invoice add up to the total value shown on the EDI invoice.
10. In situations where such missing or mismatching data is found during the edit process, the VANs usually send messages to the originator informing it about the missing/ mismatched data and the request re-transmission of the same. For example, the ASC X12, upon receipt of the shipment status message (214) with missing data, sends a status inquiry (213) transaction to the carrier requesting correction and re-transmission.
11. Validate and verify the information stored in customers' databases for missing data and send messages to appropriate firms requesting correction of the missing data.

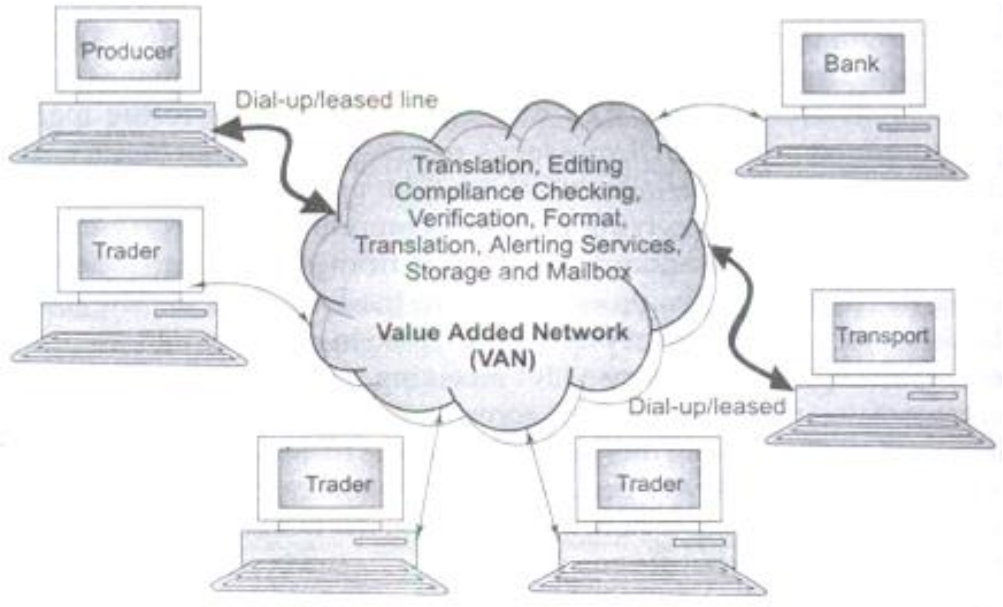


Fig 4.3 Typical VAN Example

There are many third party VAN providers the marketplace. Some of them are listed here:

1. **GEIS** - Operated by General Electric of USA, GEIS has presence in over 50 countries, GE as the major trader (buyer as well as supplier) of goods from top corporations of the world has brought major trade partners on a VAN.
2. **Cable & Wireless** - Highly reliable, with a subscriber base of over 2000 top companies of the world, cable and wireless holds nearly 8 per cent market share of the global VAN market.
3. **GNS** - It is one of the largest value added network, and has presence in around 36 countries.
4. **Transpac** - A France based EDI VAN provider, Transpac owns the largest domestic

VAN market share and has a strong presence in Europe. It uses the Infonet for offering VAN services outside the domestic domain.

5. **Infonet** - It is a VAN service jointly owned and operated by WorldComm, Singapore Telecom and Transpac. The owning organizations themselves offer VAN services in the local domains and cover rest of the world through the Infonet.
6. **Satyam Infoway** - Satyam is first private national Internet Service Provider (ISP) to offer EDI VAN services in India, in association with the Sterling Software of USA. In addition to the standard VAN services, it offers Web EDI VAN services as well.
7. **NICNet** - The National Informatics Center, an arm of Indian Ministry of Information Technology has established connectivity through 600 points in India. The NIC's network (NICNet) interconnects all the state capitals and district headquarters through its network. The NICNet in late 1999 also started offering value added network (VAN) services to facilitate and encourage EDI adoption in India. Some of the largest implementations of EDI in India, such as Indian Customs, Port Trust and Apparel Export Promotion Council use the NICNet VAN.

4.5 BENEFITS OF EDI

1. Reduces Lead Time

In the EDI environment, the exchange of documents among trading partners happens electronically through interconnected computers. The process of transferring the documents/information is instantaneous, offering weeks of time savings compared to the traditional environment that used postal/courier based exchange of printed documents. Also, the direct electronic transfer of documents between inter-organizational systems eliminates the chances of error due to re-entry of data on paper from one system to another

2. Improves Coordination with Suppliers

Traditional trading environments are often burdened with the problem of mismatched invoices, un-matching terms in quotations and purchase orders, missing invoices even after the bill for payment is received and many similar inter-business problems. On careful examination, it will be evident that much of these problems are caused either by delays in the transmission of printed documents, loss of documents in transition, or due to errors in the transcription of the printed information into the electronic form. The instantaneous transfer of business documents over the network in electronic form and confirmation of the same addresses makes it nearly impossible for documents to arrive in wrong sequence.

3. Reduces Redundancy

As all the documents exchanged between trading partners are stored in an electronic mailbox, documents can be accessed, retrieved, and examined at any point of time. Either trading partner can access, examine, and make a copy of the document from the electronic box instantly. Contrast it with the non-EDI system; it may take hours, or even days, to locate and

retrieve a printed business document from the past. Many a time, trading partners file copies of the same document at multiple places. The EDI environment eliminates the need for multiple copies and reduces redundancy without compromising the accessibility and retrieval of old documents.

4. Expands the Market Reach

Most large manufacturers like General Motors deal with EDI-enabled suppliers only. In the process of streamlining the purchase process they often institute a value-added network. By being a part of their value added network, many opportunities open up for supplying the material to some other larger suppliers who are also a part of the network. Also, with the growth of electronic commerce and further integration of EDI with electronic commerce, the creation of an electronic marketplace by large manufacturers who buy supplies from many large and small suppliers, has become a reality. By, participating in this large market place you are likely to pick many orders from other suppliers who are a part of the market/network.

5. Increases Revenue and Sales

Many large organizations use EDI and trade with other EDI-enabled suppliers. The efficiency brought about by EDI reduces the total transaction friction by eliminating paperwork and related errors that ensue. It also leads to quicker settlement of accounts. The reduced transaction friction saves money and the supplier is in a better position to offer the items at cheaper costs, leading to improved revenue realizations and sales.

6. Minimizes Transcription Errors

Since the documents are sent and received in electronic form, the need to write the data on paper is not there and, as a result, hand-written transcription errors are totally eliminated.

Direct Benefits of EDI

- Since the transfer of information from computer to computer is automatic, there is no need to re-key information. Data is only entered at the source.
- The cost of processing EDI documents is much smaller than that of processing paper documents.
- Customer service is improved. The quick transfer of business documents and marked decrease in errors allow orders to be met faster.
- Information is managed more effectively.

Strategic Benefits of EDI

- Customer relations are improved through better quality and speed of service.

- Competitive edge is maintained and enhanced.
- Reduction in product costs can be achieved.
- Business relations with trading partners get improved.
- More accurate sales forecasting and business planning is possible due to availability of information at the right place at the right time.
- There is improved job satisfaction among data entry operators, clerks, etc. when they are re-deployed in more creative activities.

4.6 APPLICATIONS OF EDI

- The ability to exchange business documents electronically has been found to facilitate coordination between business partners, reduce the lead-time and thus reduce inventory.
- Although, large manufacturing and transportation companies were the early birds who recognized the advantages, any of the other industry segments also stand to benefit from electronic document exchange.
- The health care, financial sectors and cross-border trade facilitated through electronic document exchanges are some other sectors that adopted and derived the returns from EDI.
- Banking and financial payments like Large-scale or wholesale payments (e.g., bank-to-bank transfer), Small-scale or retail payments (e.g., automated teller machines and cash dispensers) and Home banking (e.g., bill payment) are also facilitated through EDI.
- Retailing payments through Credit cards (e.g., VISA or MasterCard), Charge cards (e.g., American Express), Smart cards or debit cards (e.g., Mondex Electronic Currency Card), Token-based payment systems through Electronic cash (e.g., Digi Cash), Electronic checks (e.g.Net Cheque) etc are also done through with widely used EDI-based electronic ordering and billing processes.
- EDI software can also be used in e-mail and network services in order to send electronic purchase orders, invoices and payments back and forth.

ELECTRONIC COMMERCE - ARCHITECTURAL FRAMEWORK

5.1 FRAMEWORK OF E-COMMERCE

Electronic commerce applications require a reliable network infrastructure to move the information and execute a transaction in a distributed environment. These applications rely upon two key component technologies i.e., the publishing technology necessary for the creation of digital content and distribution technology to universally move the digital contents and transactions information. Thus, in the framework network infrastructure forms the very foundation while publication and distribution technologies are the two pillars that support the creation of distributed electronic commerce applications. In addition to technological infrastructure and applications, for electronic commerce to flourish, it is essential to have a business service infrastructure. The business service infrastructure comprises of directory services; location and search services; and a trust mechanism for private, secure, reliable, and non-deniable transactions, along with an online financial settlement mechanism.

The multi-layered architecture of electronic commerce, comprising essential blocks has been shown in Fig. 4.1.

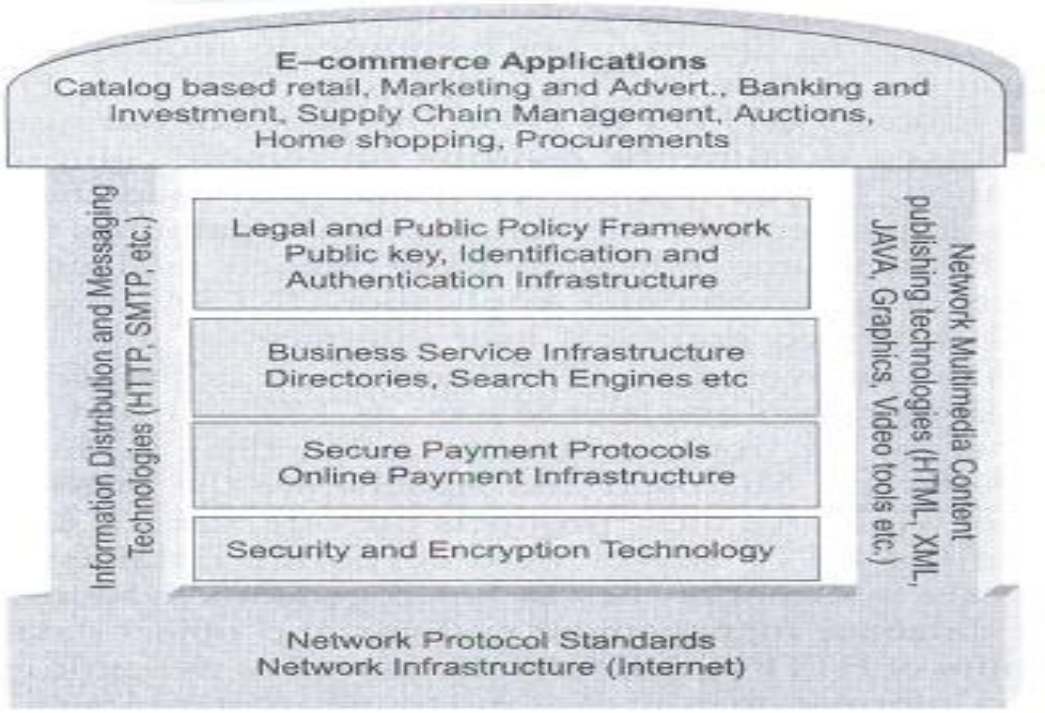


Fig. 4.1 Architectural Framework for Electronic Commerce

The framework describes various building blocks, enabled by technology, for creating new markets and market opportunities. The building elements of electronic commerce architecture are described as follows

5.1.1 Network Infrastructure

The network infrastructure forms the very basis of the electronic commerce, playing the role, in many ways, analogous to road/transport highways in the traditional commerce. Information, information goods and transactions move between the clients and commerce provider, through network highways. The network infrastructure, known as internet, consists of heterogeneous transport systems. These different transport networks interconnect using common network protocol standards called **TCP/IP**. TCP/IP is concerned with the issue of providing a reliable data transmission mechanism for applications. All the computers connected / accessible on the internet share a common name and address space which uniquely identifies the machine

The common name space is implemented using the **Domain Name System (DNS)** and ensures that each machine on the internet has a unique name. The name here refers to the combination of the host and domain name. TCP/IP named after its two primary protocols - **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**, has emerged as a de facto standard of connectivity. In TCP / IP networks, the internet protocol layer delivers the IP packets from end to end in a connectionless format. The IP layer receives packets from the upper layers and injects them into underlying networks. In IP layers each packet is delivered independent of all other packets, thus in the process it may deliver packets out of the sequence in which they were sent.

The transmission control protocol (TCP) provides a connection-oriented reliable delivery mechanism. It insures that a byte-stream, emanating at one machine destined for the other machine, is delivered without any errors, duplication and in the original sequence. TCP layer at the originating machine divides the incoming byte-stream from applications into multiple IP packets and adds sequence numbers to them. The receiving TCP process at the destination machine combines the packets together and orders them by the original sequence number assigned to them prior to delivery.

The transport layer in addition to TCP also supports a **User Datagram Protocol (UDP)**. UDP is an unreliable connectionless protocol. It is often used in applications, such as video and audio streaming, where prompt and constant delivery of data is more important than the in sequence and reliable delivery offered by TCP. It is also utilized by single packet request-reply applications, where speed of delivery is more important.

The construction of a reliable network infrastructure requires two types of hardware-transmission media and components such as routers, switches, hubs, and bridges. The network bandwidth is usually dependent upon the quality of transmission media. The coaxial cables, copper wire, fiber optical cables, radio, microwave, and satellite based transmission mechanisms are some modes utilized for the physical transmission of data. Data transmission or the bandwidth has been provided by telecom companies operating telephone lines, cable TV systems with coaxial cables, direct broadcast systems (DBS), wireless network providers, computer networking providers, satellite transponders, and fiber optical infrastructure providers. Access to the network requires devices that are referred to as Data Terminal Equipment (DTE).

5.1.2 Information Distribution Technology

Information distribution and messaging technologies provide a transparent mechanism for transferring information content over a network infrastructure layer. It is accomplished through software systems that implement **File Transfer Protocol (FTP)**, **Hypertext Transfer Protocol (HTTP)** and **Simple Mail Transfer Protocol (SMTP)** for exchanging multimedia contents consisting of text, graphics, video, and audio data. For electronic commerce, challenges exist in providing a secure, reliable, and portable mechanism that can inter-operate over a variety of devices such as personal computers, workstations, palmtops, set-top boxes and wireless communicators.

Once delivery message content has been created and stored on a server, messaging and information distribution methods, it carries that content across the network. The messages which are sent from one site to another site include purchase orders, shipping notices, invoices and other product delivery data. The messaging vehicle is called middle ware software that sits between the Web servers and the end-user applications and masks the peculiarities of the environment. Messaging and information distribution also includes translators that interpret and transform data formats.

The HTTP protocol permitted the transparent delivery of hyper-linked documents, residing on remote computers, consisting of multimedia information. The messaging service offered by SMTP servers have been implemented by the various software programs that ensure a message composed and dispatched for a specified destination address is delivered reliably. Some of the commonly used and available implementations of the SMTP services are Sendmail and Qmail programs. Similarly, various implementations of FTP protocols have also existed for quite some time and have been in use for reliably transferring files from one computer to another over the network.

5.1.3 Networked Multimedia Content Publishing Technology

The information distribution protocol, HTTP, delivers the documents written in the **Hypertext Markup Language (HTML)**, to the client program. The language offers an easy way for integrating multimedia content, residing in a variety of computers connected on the internet. HTML makes it possible to integrate the multimedia content in a document form and the integrated content then can be published using the HTTP servers. Clients can make requests, for the published information residing on HTTP servers. Clients submit requests to servers using the Hypertext Transfer Protocol. The servers respond to requests by locating and delivering the HTML document or error message to the client. The client programs, also known as browsers, parse and render the delivered HTML documents on the screen of the client machine. All published documents on the internet can be uniquely identified and located by a **Uniform Resource Locator (URL)** address. The URL address effectively serves as a unique name of the published document, worldwide.

The URL is made up of three parts: the protocol name, machine name, and the name of document on the machine. The machine name part of URL identifies the machine and protocol name determines the distribution server that will serve the document and the rules and format

in which the document will be served. The document name of the URL points to a specific document on the machine. Thus, a URL is capable of addressing as well as locating documents in the entire universe of internet.

The HTML is tag-based language and provides a rich set of tags that are used for designing the page layout, embedding multimedia objects, hyperlinking documents residing on the same as well as other internet connected machines. A simple HTML document can be developed in any standard text editor. In addition to HTML, the **Extensible Markup Language (XML)** has also emerged as a language for developing pages for the web. HTML is more concerned about how a page is formatted and displayed, while XML describes the actual content of a page. It simplifies the task of describing and delivering structured data from any application, thus, providing users with the ability to share and search the data in XML documents, in much the same way as we share and search data from databases and files. The actual multimedia content, i.e., the graphics, video clips, audio clips, and animated content can be developed by tools and editors available in the respective areas. Web technology, consisting of information distribution (HTTP) and publishing as well as integration (HTML and multimedia content editors), provides the two basic pillars on which electronic commerce applications are built.

5.1.4 Security and Encryption

Wide connectivity and ready access to information also opens up sites to unwanted intruders. For electronic commerce to be viable, two important issues need to be addressed: protection of the source of information that is being made available online, and protection of the transaction that travels over the network. The first issue is addressed by deploying strong site security measures that constantly monitor the site for authenticated and authorized activities, virus detection and elimination systems, and intrusion detection systems and firewalls. The second issue of securing the transaction, carried out over the network, requires addressing several security and confidentiality related issues. The confidentiality or privacy of the transaction data can be addressed by using various encryption techniques. The **shared key** as well as the **public/private key** pair based encryption techniques can be used for the purpose. In addition to the confidentiality of the transaction issue, the other important issues is to ensure that the messages exchanged between two parties in a transaction have not been tampered with and assure that neither of the parties will repudiate the transaction.

The process of identifying and authenticating transacting parties is essential in the electronic commerce environment. The task of authentication can be accomplished with the help of **Digital Certificates** signed/issued by a trusted certification authority. Encryption and digital signatures are used for ensuring message integrity and non-repudiation. The issue of protecting the information available on the electronic commerce site: Privacy, Secrecy and Tamper-proofing of information flow from one site to another. Encryption technologies based on shared key mechanisms such as **Data Encryption Standard (DES)** or **public-private keys** such as RSA algorithms have been utilized for addressing the issues of authentication, authorization, privacy and non-repudiation.

5.1.5 Payment Services

Online payment is fundamental to the acceptance of electronic commerce as a viable alternative to traditional commerce. It is a mechanism that facilitates an online financial exchange between concerned parties and helps users to pay for an item they have bought online. In the case of large and established businesses deploying Electronic Data Interchange (EDI) for transactions, banks have been supporting the electronic payment mechanism through the **Electronic Fund Transfer (EFT)** channel. Several scalable and flexible electronic payment mechanisms-cash, cheques and credit cards have emerged, essentially imitating traditional payment mechanisms. Electronic payment mechanisms represent currency in the form of digital bits and require security and encryption mechanisms to ensure that it cannot be duplicated, reused or counterfeited and yet can be freely exchanged. In addition, these electronic payment systems also offer the confidentiality, integrity, and privacy of traditional payment systems. The electronic payment mechanisms evolved can be classified in to three major categories-pre-paid, instant-paid, and post-paid. The instant-paid mechanism requires equivalence to Government/Central Bank backed cash transactions. None of the electronic payment systems offer the equivalence to a Government/Central Bank guarantee like cash. Debit cards come closest to instant-paid electronic payment systems. The various electronic/ digital cash mechanisms are in fact prepaid payment systems.

In these systems the physical currency is used for acquiring digital cash that in turn can be spent in an electronic payment environment. Post-paid mechanisms are equivalent to credit card and cheque based transactions Ecash, Digicash, NetBill, Micromint, Netfare and Mondex are some examples of payment systems that fall in the pre-paid category. The FSTC electronic cheque, Netcheck, and Cybercash systems are some examples of post-paid electronic payment systems. Traditional credit card majors have come up with Secure Electronic Transaction (SET) protocol. The protocol provides a secure mechanism for using standard credit cards, over the network, for electronic payment purposes.

5.1.6 Business Services Infrastructure

Business service infrastructure includes **directories and catalogues**. These are essential for identifying and locating businesses that meet customer requirements. The directories and catalogs refer to Business Directories and Yellow Pages used by customers to identify and locate businesses that are likely to provide the service or fulfill product demand in traditional commerce. Search engines and directory service providers like AltaVista, Google, Yahoo! Infospace, Bing, etc are identified and capitalized on the need by providing the service.

Search engines compile their databases by employing "robots", often called spiders, to crawl through the web space. The crawling is done by picking a page and then visiting all the links referred to in that page and in the process identifying and perusing the pages. Once the spiders get to a web site, they typically index words on the publicly available pages at that site. The engine scans its index for matching the key words and phrases typed by the user. The search engine maintains a database that contains correspondence between text terms and document URLs. Finally the search engines return the relevant URLs for the keywords or

search terms entered by users. With millions of web pages on the internet, a simple search for any term or phrase may result in thousands of URLs. Thus, it is important for web site designers that their URL is ranked amongst the top few for the relevant terms and keywords.

A hierarchical directory structure that classifies web sites based on the content in various categories, subcategories and further granularity of the same has been alternatively used for successfully locating the relevant information. Many a time the entry in the directory and within that appropriate category is done after reviewing the content of a web site. This allows users to locate the relevant web site by navigating through the hierarchy.

5.1.7 Public Policy and Legal Infrastructure

The access to network infrastructure and legal framework, for the protection of transactions conducted over the network, play important role in the viability and the growth of electronic commerce. In many of the countries the government is the only provider of telecommunication access, which has inhibited the growth of the network infrastructure in many countries. The telecommunication infrastructure designed for the voice data can carry data traffic only to a limited extent. Universal access at an affordable cost is important for the growth of the digital economy and electronic market. The Organization of Economic Cooperation and Development (OECD) have been putting together several initiatives and policy guidelines to address communication infrastructure development throughout the world.

Although, security and encryption technology can help in ensuring the secrecy and integrity of data, to ensure that the transaction is conducted on behalf of two acclaimed parties, an authentication infrastructure has to be put in place. Authentication is offered by a third party that certifies the identity of the transacting parties. In traditional commerce people usually prefer doing business within the neighborhood or at well known shopping centers with businesses whose reputations they trust. To provide a legal framework for ecommerce transactions, the General Assembly of the United Nations adopted a Model Law on Electronic Commerce in 1997 which recommended that all the member states should favorably consider the Model Law in the exchange and storage of business transaction information.

The Controller of Certification Authorities (CCA) is responsible for issuing licenses to and for regulating the certification authorities in India and maintains a directory of all the certificates as well. Thus the certification authority, based on public key infrastructure of CCA provides legal policies and framework provided with digitally signed contract that ensures non-repudiation of contracts, purchase orders and agreement repositories.

MULTIPLE CHOICE QUESTIONS

Questions for Understanding

a. What do you think PR stands for?

A. Purchase request

B. Purchase requisitions

C. Purchase receipt

D. Purchase report

b. What do you think EDI stands for?

A. Electronic Data Information

B. Electronic Data Insurance

C. Electronic Data Interchange

D. Electronic Data Independent

c. What do you think EFT stands for?

A. Electronic Fund Transport

B. Electronic Fund Texting

C. Electronic Fund Technology

D. Electronic Fund Transfer

d. Can you clarify full form of DISH?

A. Data Interchange for Shopping

B. Data Interchange for Selling

C. Data Interchange for Shipping

D. Data Interchange for Securing

e. Can you clarify full form of ANSI?

A. American National Standards Interchange

B. American National Standards Information

C. American National Standards Infrastructure

D. American National Standards Institute

f. Can you clarify full form of Expand ISO?

A. International Standards Organization

B. Internal Standards Organization

C. Information Standards Organization

D. Institutional Standards Organization

g. Can you clarify full form of TDI?

A. Traditional Data Interchange

B. Trade Data Interchange

C. Temporal Data Interchange

D. Transport Data Interchange

h. Can you clarify full form of FTP?

A. File Text Protocol

B. File Transport Protocol

C. File Transfer Protocol

D. File Trait Protocol

i. Can you clarify full form of HTTP?

A. Hyper Transaction Transfer Protocol

B. Hyper Trait Transfer Protocol

C. Hyper Time Transfer Protocol

D. Hyper Text Transfer Protocol

j. Can you clarify full form of VAN?

A. Value-artificial network

B. Value-action network

C. Value-added network

D. Value-access network

k. What do you think DISA stands for?

A. Data Interchange Standards Association

B. Data Interchange Standards Application

C. Data Interchange Standards Accessories

D. Data Interchange Standards Arrangement

l. What do you think, _____ refers to the network infrastructure that is used for the exchange of information between trading partners.

A. Interconnection layer

B. Internal layer

C. International layer

D. Information layer

m. What do you think, systems used by financial institutions are a prime example of the application of EDI in the banking and financial sector.

A. EDI

B. EFT

C. ECG

D. EGG

Questions for Application

n. Do you know, which process defines the relationship between a manufacturing organization and a consumer organization.

A. Typical trading

B. Conditional trading

C. Computer trading

D. Illegal trading

o. Do you know, _____ is the exchange of business documents between any two trading partners in a structured, machine-readable form.

A. EDI

B. EFT

C. ECG

D. EGG

p. Can you tell what is defined as any transfer of funds initiated through an electronic terminal, telephonic instrument, or computer to order, instruct or authorize a financial institution to debit or credit an account.

A. EDI

B. EFT

C. ECG

D. EGG

q. Do you know, The general architecture of the EDI system consists of how many layers.

A. Two

B. Four

C. Six

D. Eight

r. The shipping industry devised a set of standards called _____.

A. Data Interchange for Shopping

B. Data Interchange for Selling

C. Data Interchange for Shipping

D. Data Interchange for Securing

s. Do you know, which standard is promoted by the United Nations Economic Commission, which is responsible for the adoption and standardization of messages.

A. EFTFACT

B. EDIFACT

C. ECGFACT

D. EDDFACT

t. Do you know, what is a convenient method for conducting EDI which provides functionalities related to connectivity and common services?

A. Value-artificial network

B. Value-action network

C. Value-added network

D. Value-access network

u. Do you know, The different transport networks interconnect using common network protocol standards is called as _____.

A. TCP/UP

B. TCP/UDP

C. TCP/DNS

D. TCP/IP

v. Can you tell, The common name space is implemented using the _____ and ensures that each machine on the internet has a unique name.

A. Domain Name System (DNS)

B. Digital Name System (DNS)

C. Demand Name System (DNS)

D. Data Name System (DNS)

w. What do you think, all published documents on the internet can be uniquely identified and located by an _____ address.

A. United Resource Locator (URL)

B. Uniform Resource Locator (URL)

C. Union Resource Locator (URL)

D. Ultra Resource Locator (URL)

x. Can you tell, Business service infrastructure includes _____?

A. Dictionaries and categories

B. Direction and categories

C. Directories and catalogues

D. Dictionaries and catalogues

y. Do you know which of the following is responsible for issuing licenses to and for regulating the certification authorities in India and maintains a directory of all the certificates as well?

A. Control of Certification Authorities (CCA)

B. Connection of Certification Authorities (CCA)

C. Categories of Certification Authorities (CCA)

D. Controller of Certification Authorities (CCA)

Long Answers

Questions for Understanding

1. Write in your own words about Electronic Data Interchange and Electronic Fund Transfer.
2. Illustrate various services provided by VAN.
3. Explain the role of online payment system in E-commerce.
4. Can you explain the services provided by networked multimedia content publishing in e-commerce.
5. Illustrate different protocols and their services in the network service infrastructure.
6. Illustrate the essential technologies for ensuring security in an e-commerce environment.

Questions for Application

1. Analyse the building blocks of EDI system with a diagram.

2. Analyse the framework of e-commerce with a neat diagram.
3. List and analyse benefits of EDI system.
4. What are some of the direct benefits and strategic benefits of EDI.
5. What are the different application of EDI.
6. Analyse the role of business service infrastructure in E-Commerce.

UNIT IV

ELECTRONIC COMMERCE: SECURING THE BUSINESS ON INTERNET

6.1 INTRODUCTION

A fundamentally insecure infrastructure and an extremely dynamic environment in terms of both topology and emerging technology-make network defence extremely difficult. Because of the inherent openness of the internet and the original design of the protocols, internet attacks in general are quick, easy, inexpensive, and many a time hard to detect or trace. Attacks can be launched readily from any remote corner of the world, with the location of the attacker being easily hidden. Anyone can "break-in" to a site and gain privileges on that site to compromise confidentiality, integrity, or availability of its information or services. In spite of this, it is common for sites to be ignorant of the risks or unconcerned about the amount of trust they place in the internet. They are blissfully unaware of what can happen to their information and systems, and are under the illusion that their sites will not be targeted, or that precautions they have taken are sufficient. Because technology is constantly changing and intruders are constantly developing new tools & techniques, solutions do not remain effective indefinitely.

Since much of the traffic on the internet is not encrypted, confidentiality and integrity are difficult to achieve. This situation undermines not only applications, but also more fundamental mechanisms such as authentication and non-repudiation. As a result, sites may be affected by a security compromise at another site, over which they have no control. Another factor that contributes to the vulnerability of the internet is the unplanned growth and use of the network, accompanied by rapid deployment of network services, and involving complex applications. The swift emergence of new products, in the rush to capture a share of the lucrative market, has compromised the security, because these services are not designed, configured, or maintained securely. Finally, the explosive growth of the internet has expanded the lack of well-trained and experienced people to engineer and administer the network in a secure manner, opening up opportunities for the intruder community.

6.2 SITE SECURITY POLICIES

The following classification helps in identifying the technical failures behind successful intrusion techniques as well as the means of addressing these problems.

1. Flaws in Software or Protocol Designs

Protocols define the rules and conventions for computers to communicate on a network. A protocol having a fundamental design flaw is inherently vulnerable to exploitation, no matter how well it is implemented. An example of this is the Network File System (NFS), which allows systems to share files. This protocol does not provide for authentication; there is no way of verifying that a person logging in really is whom he or she claims to be. This security lapse makes NFS servers targets of the intruder community. When software design specifications are written, security is often left out of the initial description and is added to the system at a later stage resulting in unexpected vulnerabilities.

2. Weaknesses in Implementation of Protocols and Software

Even when a protocol is well designed, it can be vulnerable because of the way it is implemented. For example, an electronic mail protocol may be implemented in a way that permits intruders to connect to the mail port of the victim's machine and fool the machine into performing a task not intended by the service. If intruders supply certain data to the "To:" field, instead of a correct e-mail address, they may be able to fool the machine into sending them confidential information about the user and password as well as access to the victim's machine, with privileges to read protected files or run programs on the system. This type of vulnerability enables intruders to attack the victim's machine from remote sites, without access to an account on the victim's system. Many a time bugs in the software are detected only after the software is released, making the systems, on which the applications are being run, vulnerable. This provides the intruders with a range of opportunities for exploiting the weaknesses, using various attack tools. By exploiting program weaknesses, intruders at a remote site can gain access to a victim's system. Even if they have access to a non-privileged user account on the victim's system, they can often gain additional unauthorized privileges and wreak the system.

3. Weaknesses in System and Network Configurations

Vulnerabilities in the category of system and network configurations may not be caused by problems inherent in protocols or software programs. Rather, vulnerabilities are a result of the way these components are set up and used. Products may be delivered with default settings that intruders can exploit. System administrators and users may neglect to change the default settings, or they may simply set up their system to operate in a way that leaves the network vulnerable. An example of a faulty configuration that has been exploited is anonymous File Transfer Protocol (FTP) service. Secure configuration guidelines for this service stress the need to ensure that the password file, archives tree, and ancillary software are separate from the rest of the operating system, and that the operating system cannot be reached from this staging area. When sites misconfigure their anonymous FTP archives, unauthorized users can get authentication information and use it to compromise the system.

6.2.1 TYPES OF SECURITY BREACH INCIDENTS

There are different types of Security Breaches that may occur at a site. Some of the common network security incidents are defined as follows:

- **Probe:** A probe is characterized by unusual attempts to gain access to a system, or to discover information about the system. One example is an attempt to log in to an unused account.
- **Scan:** A scan is simply a large number of probes, done by using an automated tool like continuously generating some random password and trying to login to a system.
- **Account Compromise:** An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system level or root level privileges. It might expose the victim to serious data loss, data theft, or theft

of services.

- **Root Compromise:** A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term 'root' is derived from an account on UNIX systems, that typically has unlimited, or "superuser", privileges. Intruders who succeed in a root compromise have the entire system at their mercy and can do just about anything on the victim's system, including running their own programs and even changing the way the system works.
- **Packet Sniffer:** A packet sniffer is a program that captures data from information packets, as they travel over the network. This data may include user names, passwords, and proprietary information that travels over the network in unencrypted format. With perhaps thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems.
- **Denial of Service:** The goal of the denial-of-service attack is to prevent legitimate users from using a service. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data, or deliberately consume a scarce or limited resource such as process control blocks or pending network connections. They may also disrupt the physical components of the network or tamper with data in transit, including encrypted data.
- **Exploitation of Trust:** Computers connected via networks enjoy privileges or trust relationships with one another. For example, the computer checks a set of files that specify which other computers, on the network are permitted to use those commands before executing some commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.
- **Malicious Code:** Malicious code is a generic term for programs that cause undesired results on a system when executed. Such programs are generally discovered after the damage is done. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that the attackers have altered. These altered files produce unintended additional effects whenever they are rendered or executed. Worms are self-replicating programs that spread without any human intervention, after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These of programs can lead to serious implications like data loss, denial of service, and other types of security incidents

Protecting the network

A security policy is a formal statement of the rules by which people with access to an organization's technology and information assets must abide, to ensure the security of. There are two conflicting, underlying philosophies that can be adopted when defining a security plan. The choice between them depends on the site and its needs for security.

1. The **"deny all"** model suggests turning off all services and then selectively enabling services on a case by case basis as required. This can be done at the host or network

level, as appropriate. This model is generally more secure than the next one. However, more work and a better understanding of services is required to successfully implement a "deny all" configuration.

2. The **"allow all"** model is based on the logic of simply turning on all services, usually with the default at the host level; and allowing all protocols to travel across network boundaries, usually with the default at the router level. As security gaps become apparent, they are restricted or patched at either the host or network level. This model is much easier to implement, but is generally less secure than the "deny all" model. Each of these models can be applied to different portions of the site, depending on factors like functionality requirements, administrative control, and site policy. For example, an "allow all" policy may be adopted for traffic between a LAN's internal to the site, but a "deny all" policy can be adopted between the site and the internet.

6.3 Protecting the Network

As stated earlier, networks are vulnerable to several types of security attacks. The following are some of the common attacks and prevention mechanism associated with them.

1. Denial of Service (DOS)

The denial of service attack brings the network to a state in which it can no longer carry legitimate users' data. The two common weaknesses that the "denial of service" attackers exploit in carrying out the attack on a site are as follows:

1. Attacking routers
2. Flooding the network with extraneous traffic

An attack on the router is designed to cause it to stop forwarding packets, or forward them improperly. In a flood attack, the router is bombarded with unroutable packets, causing its performance to degrade.

How to Prevent Denial of Service?

The solution to most of these problems is to protect the routing update packets sent by the routing protocols in use. There are three levels of protection

1. **Clear-text password:** Passwords only offer minimal protection against intruders who do not have direct access to physical networks. Passwords also offer some protection against misconfigured routers. The advantage of passwords is that they have very low overheads, in both bandwidth and CPU consumption.
2. **Cryptographic checksum:** Checksums are some codes which you can add to the message which can only be identified by the receiver of the message. If the receiver gets the correct checksum after calculation, he is confirmed that the message has not been changed by any intruder or hacker. This helps to protect against the injection of spurious packets, even if the intruder has direct access to the physical network.
3. **Encryption:** Maximum security is provided by complete encryption of sequenced or uniquely identified, routing updates. This prevents an intruder from determining the

topology of the network. The disadvantage of encryption is the overhead involved in processing updates.

2. Sniffing

Sniffing uses network interface to receive data intended for other machines in the network. For example a bridge connects two network interfaces by retransmitting the data frames received on one interface to the other. Thus, in this process it examines all the frames. The "network analyzer" is a device that can receive all the traffic on the network for diagnostic and analytical purposes or diagnosing a variety of problems. This performs a useful function; but the same capability can be exploited by a person with malicious intentions, to tap the information.

Sniffing data from the network leads to leakage of several kinds of information that should be kept secret for a computer network to be secure. Through the use of sniffers the critical information such as passwords, financial account numbers, confidential or sensitive data and low level protocol information can be tapped. Although, computer systems mask the password when the user types it on the screen, they are often sent as clear text over the network which can be easily seen by any ethernet sniffer providing the intruder access to confidential or sensitive data. In businesses that conduct electronic funds transfers over the internet, many transactions involving the transmission of financial account numbers, such as credit card numbers and account numbers can be picked up by the sniffer device. The interceptor can use this information to access or even transfer funds from user's account.

How to Prevent Sniffing?

Sniffing can be prevented or at least its effects can be mitigated, through the proper understanding of these devices and deploying them in an appropriate configuration. Encrypting all the message traffic on the network ensures that the sniffer will only be able to get the encrypted text (chiper text) rather than the clear text information. The information will remain protected, provided the encryption mechanism deployed is strong enough and cannot be easily broken. In an environment where all computers are connected on a single LAN segment, we can define a secure LAN segment, whose data frames do not reach other LAN segments. Active hubs can also be configured to send only frames meant for a specific machine and line. In this configuration, no machine gets an opportunity see the frames meant for other machines.

Kerberos is another package that encrypts account information going over the network. It comes with a stream-encrypting remote login (rlogin) shell and stream-encrypting remote terminal (telnet) program. This prevents intruders from capturing the actions of the user, after he logs in. Some drawbacks of kerberos are that all the account information is held on one host, and if that machine is compromised, the whole network is rendered vulnerable.

The information can also be protected from sniffing based attacks by employing a zero-knowledge/ password authentication technique. This method is used for secure authentication without password usage. Networks that use this system have a client and a server that share a

very long sequence of digits. During the client request for connection to a server, the server asks the client for a set of digits, in a small set of positions in the sequence. Since the no. of digits in the sequence is very long, the knowledge of a few digits is not sufficient for using it in a future attack, as the server inquires a different set of positions each time the client connects.

INTRODUCTION TO CYBER SECURITY

What is Cyber Security?

Cyber Security involves protecting key information and devices from cyber threats. It is a critical part of companies that collect and maintain huge databases of customer information, social platforms where personal information are submitted and government organizations where secret, political and defense information are involved. It describes how personal and key government data is protected against vulnerable attacks that possess threat to important information, may it be on the cloud, across various applications, networks and devices. Lot of money are invested in protecting all this information in an online platform. With the number of people accessing the information online increasing each day, threats to the information are also increasing, with the cost of online crimes estimated in billions.

Types of Cyber Security

Cyber Security is classified into the following:

- **Information security**
- **Network security**
- **Application security**

- **Information security** – Information security protects your information from unauthorized access, identity theft and protects the privacy of information and hardware that use, store and transmit data. Examples of Information security: Authorization of user and Cryptography.
- **Network security** – Network security protects the usability, integrity and safety of a network, associated components, connection and information shared over the network. When you secure a network, potential threats are identified and nullified from entering or spreading on the network. Examples of Network Security: Anti-virus and anti-spyware, using Firewall to block unauthorized access to your network and using Virtual Private Networks (VPNs) for a secure remote access.
- **Application security** – Application security protects applications from threats that occur due to the flaws in application design, development, installation, upgrade or maintenance phases.

Defining Security

Cybersecurity is the protection of internet-connected systems, including hardware,

software and data, from cyberattacks. In a computing context, **security** comprises **cybersecurity** and physical **security** both are used by enterprises to protect against unauthorized access to data centres and other computerized systems.

Security Goals

- Integrity
- Confidentiality
- Availability

- **C.I.A.**

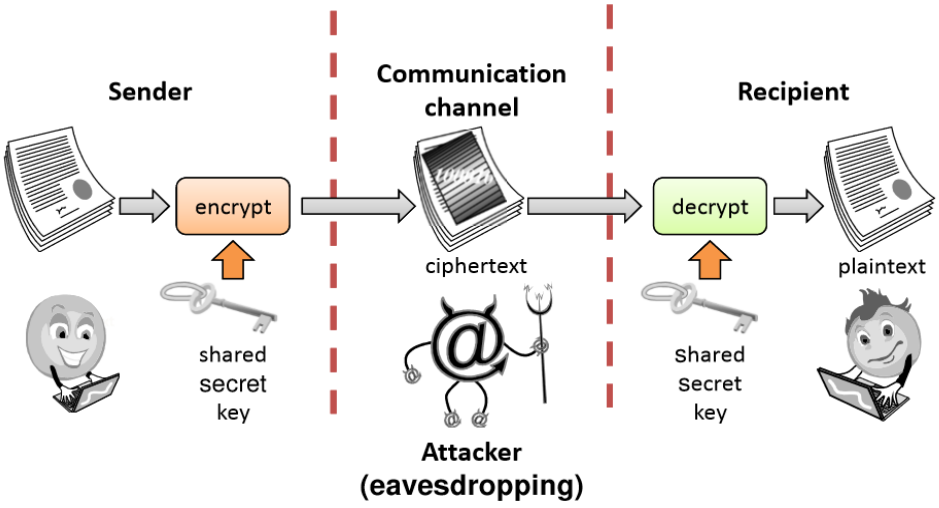
Confidentiality

Confidentiality is the avoidance of the unauthorized disclosure of information. – confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

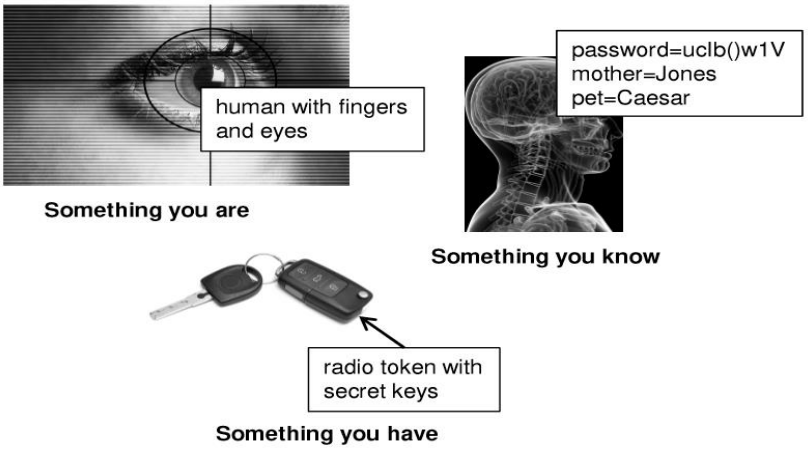
Tools for Confidentiality

- **Encryption:** The transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key).

.



- **Authentication:** The determination of the identity or role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of –something the person has (like a smart card or a radio key fob storing secret keys), –something the person knows (like a password), –something the person is (like a human with a fingerprint).



- **Authorization:** The determination if a person or system is allowed access to resources, based on an access control policy. –Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.

Integrity

The property that information has not be altered in an unauthorized way.

Tools for integrity:

- **Backups:** The periodic archiving of data.
- **Checksums:** The computation of a function that maps the contents of a file to a

numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value. –Data correcting codes: methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Availability:

The property that information is accessible and modifiable in a timely fashion by those authorized to do so.

Tools: –

- Physical protections: infrastructure meant to keep information available even in the event of physical challenges.
- Computational redundancies: computers and storage devices that serve as fallbacks in the case of failures

SECURING NETWORK TRANSACTIONS

7.1 TRANSACTION SECURITY

In E-Commerce the transaction takes place over the network. The information transmitted over the public network can be tapped, intercepted, diverted, modified by an intruder to gain benefit or cause damage to the competing business. The intruding activities can be broadly classifed into 2 categories.

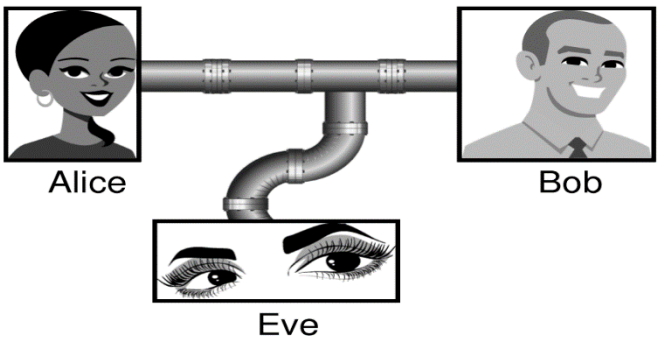
1. Passive intrusion
2. Active intrusion

In passive intrusion, the motive of the attacker is to obtain the information which is being transmitted. In passive attack, the privacy and confidentiality of information is lost but the data is not altered.

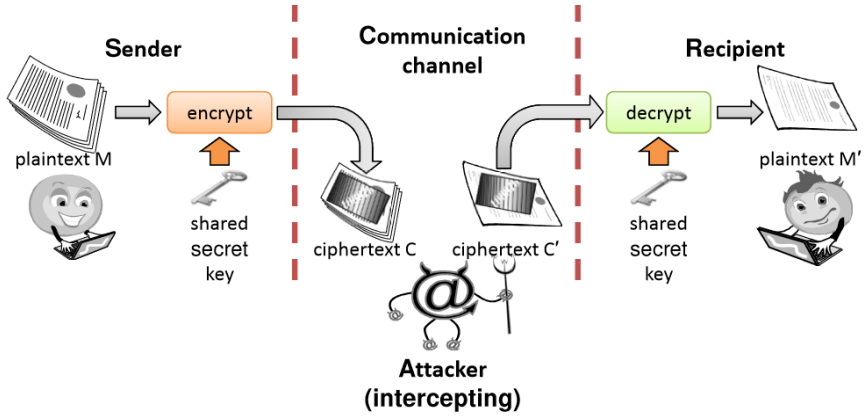
Active attackers involve mutation of data or generation of duplicate messages. Here the attacker's intention is to preventing messages from reaching the destination to masquerade as another entity and get access to restricted information.

7.2 THREATS AND ATTACKS

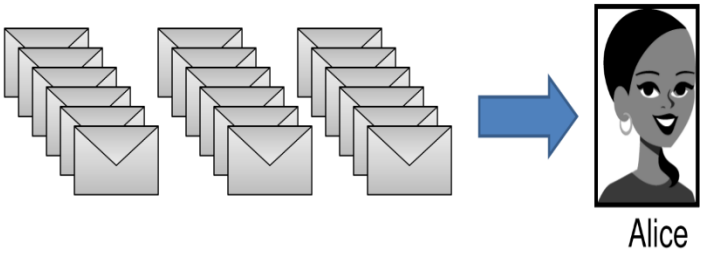
- **Eavesdropping:** The interception of information intended for someone else during its transmission over a communication channel



- **Alteration:** Unauthorized modification of information. –Example: the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted.



- **Denial-of-service: T**he interruption or degradation of a data service or information access. Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server.



- **Masquerading:** The fabrication of information that is purported to be from someone who is not actually the author.

- **Repudiation:** The denial of a commitment or data receipt. This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.

7.3 NETWORK TRANSACTION SECURITY ISSUES

The following attacks can be identified.

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Content modification:
5. Sequence modification
6. Timing modification
7. Repudiation

1. **Disclosure:** Release of message contents to an unauthorized person who is not supposed to see them.
2. **Traffic analysis:** It refers to the discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections can be determined. In either a connection oriented or connectionless environment, the number and length of messages between parties could be determined.
3. **Masquerade:** It refers to the insertion of messages into the network from a fraud source. This includes the creation of messages by an opponent that are supposed to come from an authorized entity. This also includes some fraud acknowledgment of message receipt by someone other than the valid message recipient.
4. **Content modification:** Changes to the contents of a message including insertion, deletion, transposition or modification.
5. **Sequence modification:** It refers to the modification of the sequence of messages between parties, including insertion, deletion and recording of some sequenced packets by the intruder during transmission.
6. **Timing modification:** It refers to delayed messages or replay of old message sequences that were recorded by intruder in an earlier transaction. In a connection oriented application, an entire session and sequence of messages corresponding to a full session could be recorded by an intruder and later replayed. The destination may think of it as a valid session and carryout the indicated transactions once more.
7. **Repudiation:** It refers to the refusal of the receipt of message by the destination or the refusal of transmission of message by the source.

7.4 SECURITY SERVICES

In the transactional internet environment, it is important to ensure the security of transactions as they travel over the network. In E-Commerce environment for transactions to take place, the following 5 issues are important.

1. **Authentication**
2. **Integrity**
3. **Non-repudiation:**
4. **Confidentiality:**
5. **Authorization**

1. **Authentication:** Authentication is the process of verifying the identity of a person from whom the communication message originated. There should be a mechanism to authenticate user before giving him/her access t required information.
2. **Integrity:** Information should not be altered during its transmission over the network. An intruder should not be able to add, delete or modify any part of the message during transmission.
3. **Non-repudiation:** It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

4. **Confidentiality:** Information should not be accessible to unauthorized person. It should not be intercepted during transmission. Confidentiality ensures that the contents of a message are not leaked or revealed to a hacker as it travels to its destination.
5. **Authorization:** The authentication process ensures the correct identification of the user and letting the user to login but all the information on a system may not be shared with all users. Authorization means granting permission to a person or a process to do certain things. Authorization makes sure that the user is who he claims to be.

7.5 CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography includes techniques such as microdots, merging words with images and other ways to hide information in storage and transit. Cryptography is associated with scrambling plaintext (means ordinary text sometimes referred to as clear text) into cipher text (a process called encryption) then back again.

Encryption

It is the conversion of electronic data into another form called cipher text, which cannot be understood by anyone except authorized parties. Cipher text is the encrypted text. Plain text is what we have before encryption and cipher text is the encrypted text. Cryptographic systems can be classified along 3 independent dimensions.

1. **The methodology used in transforming the plaintext to cipher text:** Encryption algorithms are based on 2 general principles.
   a. **Substitution:** Individual elements in the plaintext are mapped into another element or a group of elements by using a chart or a fixed pattern in order to disguise them.
   b. **Transposition:** The individual elements of the plaintext are rearranged.

2. **The number of keys employed by the algorithm.**
   a. **Symmetric, shared key or conventional encryption:** In this, the same key is shared by both the sender and the receiver i.e the same key is used for encryption and decryption.
   b. **Asymmetric, two way or public key encryption:** The sender uses one key for encryption and the receiver uses another key for decryption.

3. **The manner in which the original plaintext is processed**
   a. **Stream cipher:** In a stream cipher each plaintext digit is encrypted one at a time, to give a digit of the cipher text stream.
   b. **Block cipher:** This operates on fixed length groups of bits called blocks.

Cryptanalysis

A cryptosystem or cipher system is a method of disguising messages so that only certain people can see through the disguise. It is usually a whole collection of algorithms. Cryptanalysis is the art of breaking cryptosystems and seeing through the disguise. Simply put, cryptanalysis is the process of attempting to discover the plaintext message P or the key K or both. The strategy employed by the cryptanalyst depends on the nature of the encryption scheme and the information available to him. There are 2 types of Cryptosystems:

1. Conventional or Symmetric Encryption Model

In the conventional encryption model depicted in Figure 8.1 the original intelligible message (plaintext) is converted into a coded message (ciphertext).

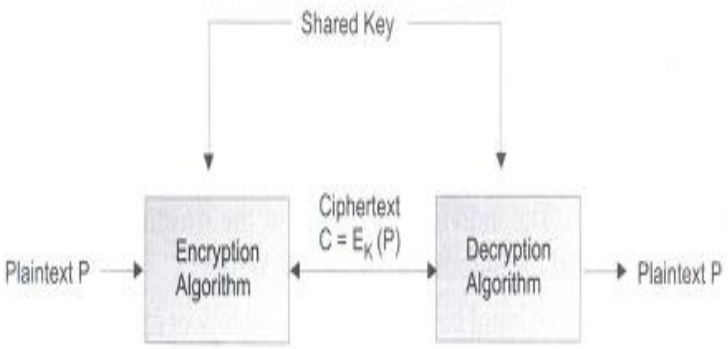


Fig 8.1 Simplified Model of Conventional Encryption

The encryption process consists of an algorithm and a key. The key is a value, which is independent of the plaintext that controls the algorithm. The output of the algorithm is dependent on the specific key being employed at the time of deciphering.

The ciphertext generated is transmitted over the network. At the receiving end, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm, and the same key that was used for encryption. Mathematically, this model can be explained as follows:

- The plaintext P is encrypted by algorithm E and the key K to ciphertext C. The key K is kept secret.
  $C = E_K(P)$.
- The decryption algorithm is used to translate the ciphertext to plaintext using same key K.
  $P = D_K(C)$.
- E & D are mathematical functions or algorithms that encrypt and decrypt for the given key K
- Since the same key is being used to encrypt and decrypt original messages. It implies that
  $P = D_K(E_K(P))$.

2. Public Key or Asymmetric Cryptosystems

Public Key cryptosystems are also called **asymmetric** two key algorithms because two different keys are used for encryption and decryption of the messages. It is computationally infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and the encryption key. In short, for each public key there is a corresponding private key and the two keys together form a unique pair. Each end system in a network has a pair of keys to be used for encryption and decryption of messages that it is going to receive. Each system publishes its encryption key known as public key by placing it in a public register or file where it is accessible to all. The companion key to be used for decryption is known as the Private Key and is kept a secret.

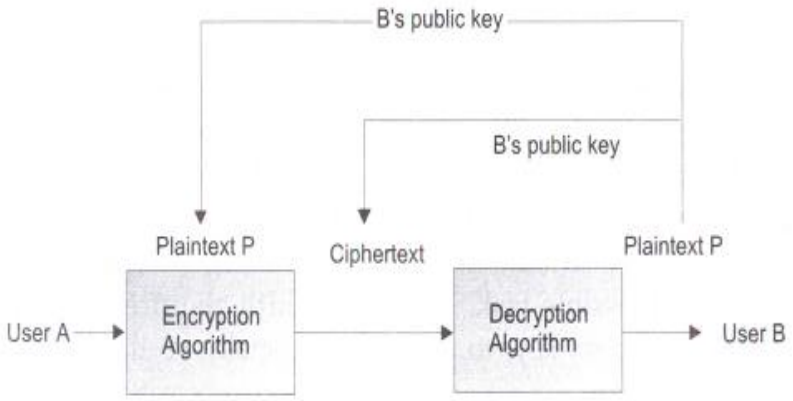


Fig 8.2 Simplified Model of Public Key Encryption

The steps in a communication sequence are as follows:

- A wants to send the plaintext P to B. B has a related pair of keys: a public key EB which is available publicly, and a private key DB, known only to B. A encrypts P with EB to generate ciphertext $C = E_{EB}(P)$, and sends the result to B.
- B, on receiving this message, decrypts it with his private key DB to retrieve the plaintext $P = E_{DB}(C)$
- Since the original message P is retrieved from the ciphertext by the decryption operation, it follows that $P = E_{DB}(E_{EB}(P))$.

Comparison of Conventional and Public Key Encryption System

Conventional Encryption	Public Key Encryption
In order to work it needs: 1. The same algorithm with the same key to be used for both encryption and decryption. 2. The sender and the receiver sharing the algorithm and the key.	**In order to work it needs:** 1. One algorithm to be used for encryption and decryption with a pair of keys - one for encryption and other for decryption. 2. The sender and the receiver each to be in possession of one of the matched pair

	of keys.
In order to ensure security: 1. The key must be kept secret. 2. To decipher a message if no other information is available should be impossible 3. Algorithm knowhow and samples of the ciphertext must not compromise on the key.	**In order to ensure security**: 1. One of the two keys must be kept secret. 2. To decipher a message, if no other information is available, should be impossible 3. Algorithm knowhow along with one of the keys and samples of the ciphertext must not lead to the determination of the other key.
Problems: 1. Keys distribution is a problem. The secrecy of entire algorithm lies on the key remaining a secret. For encryption systems all over the world, secure distribution amounts to an impossible task. 2. Unmanageable key space. If the use of a separate key for each pair of users in the network is assumed then the total number of keys is proportional to n^2 which is very large when n gets large	**Problems:** 1. Public Key cryptosystems are slow and symmetric algorithms have been observed to perform times faster than public key systems. 2. It is vulnerable to chosen plaintext attacks. If C = E(P), when P is one plaintext texts, then a cryptanalyst has to encrypt all n possible plaintexts and compare the results to C. This way one cannot get the decryption key but he surely can get P.

7.5 DIGITAL SIGNATURES

The digital signature is to the electronic world what the handwritten signature is to the traditional commerce. It must incorporate the following properties:

- It must be able to verify the author, the date, and the time of the signature.
- It must be able to authenticate the contents, at the time of the signature.
- It must be verifiable by third parties, in case of any dispute.

The above properties place the following requirements on the digital signature:

- The signature must be a bit pattern that is dependent on the message being signed.
- To prevent forgery and denial, the signature must use some information unique to the sender.
- The digital signature must be easy to generate.
- The storage of a copy of the digital signature must be simple.
- Forging the signature must be computationally infeasible, i.e., either by constructing

a fraudulent signature for a given message or constructing a new message with an existing signature.

- The signature must be easy to recognize and verify.

In this method the hash algorithm, which is a public information is used to generate a unique message digest or hash value, which is used to encrypt the data. Anyone may be able to alter the data and recalculate a new 'correct' message digest .To rectify this situation, the message digest is encrypted using a private key of the sender. This encryption of the message digest is called a 'digital signature'. Because a digital signature is created by using public key cryptography, it is possible to identify the sender of the payment information. Since the encryption is done by using the private key of a public/private key pair, this means only the owner of that private key can encrypt the message digest. Therefore, if the decryption's digital signature equals the message digest calculated by the receiver, then the payment information could not have come from anyone but the owner of the private key.

Secret Key Signatures

This approach involves a central authority that is trusted by everybody. Each user shares his/her secret key with the Certification Authority (CA).

Alice wants to send a signed plaintext to Bob. She generates the string (B, R_A, t, P) where B is the receiver Bob, P is the plaintext, t is the time-stamp and R_A is the random number and then encrypts it with her secret key K_A. This, along with her identity, is sent to CA as message 1. The CA, on observing the message from Alice, decrypts it with her key K_A and extracts the plaintext P, time-stamp t and the random number R_A. CA then combines these strings and signs it with its own signature K_{CA}. This encryption, along with A, R_A, t and P, is again scrambled using Bob's secret key to form the message 2 and this is sent to Bob.

Bob decrypts it with his secret key, K_B to extract P and K_{CA} (A, t, P). The signed message from CA is stored by Bob as a proof that Alice had sent P to Bob. In case of any dispute, when Bob claims to have received the message from Alice and she denies it, the CA can decrypt the K_{CA} (A, t, P) portion of the message received by Bob and verify the fact that the message was indeed sent by Alice to Bob.

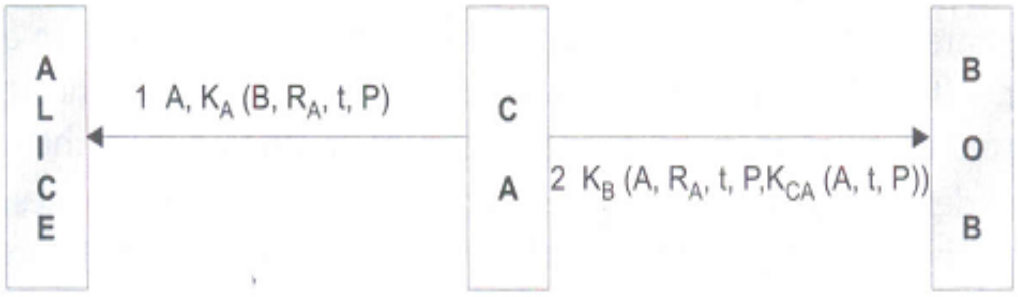


Fig 8.11 Digital Signature Using Central Authority

Public Key Signatures

If Alice wants to send the plaintext message P to Bob, by encrypting it with her private key D_A and then encrypting it with Bob's public key E_B, the message generated will be

$E_B(D_A(P))$, and this is transmitted over the network to Bob.

Bob, on receiving this message, first decrypts the message using his private key, D_B, to extract $D_A(P)$. This is then decrypted using Alice's public key, E_A, to retrieve the original plaintext P. If Alice subsequently denies having sent the message, Bob can produce both P and D_A (P). It can be easily verified that Bob has a valid message encrypted by D_A, by applying, EA, to it. The only way Bob could have received a message encrypted by D_A is by Alice sending it.

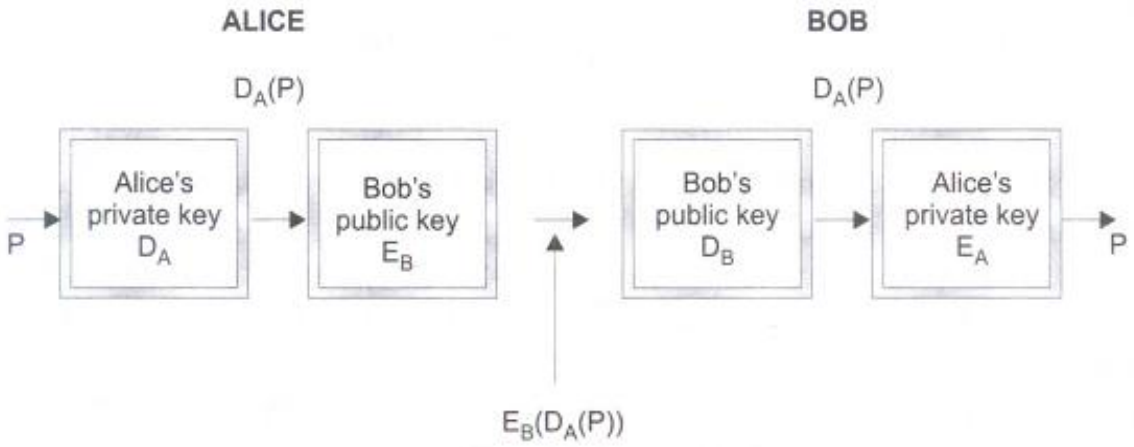


Fig 8.12 Digital Signature Using Public Key Cryptography

8.6 EMAIL SECURITY

Electronic mail, better known as e-mail, is the most widely used network based application on the internet. It is widely used across all architectures and vendor platforms. With the explosively growing reliance on e-mail for every conceivable purpose, the demand for authentication and confidentiality services has also grown. Two schemes that are extensively used to ensure the privacy of e-mails are:

a. Pretty Good Privacy (PGP)
b. Privacy Enhanced Mail (PEM)

PGP

Pretty Good Privacy is a comprehensive e-mail security package that addresses privacy, authentication, confidentiality, digital signatures and compression issues.

Mechanism of PGP: Alice intends to send the plaintext message P, to Bob, in a secure manner. The public and private keys of Alice are E_A and D_A, respectively. For Bob the corresponding keys are E_B and D_B.

Alice types the message P and runs the PGP program on her workstation. The program hashes the message P using MD5 and then encrypts the result with Alice's private RSA key, D_A. The encrypted hash and the original message are concatenated into a single message P' and compressed using the ZIP program, resulting in output P'.zip. Alice, on being prompted by the PGP program enters a random input. The content and the typing speed are used to generate a 128-bit IDEA message key, K_M. The P'.zip is encrypted using the newly generated key, with IDEA in cipher feedback mode. K_M is encrypted with Bob's public key, E_B. The two components are concatenated and converted to base-64. The resulting message then contains letters, digits and the symbols like +, / and =, and is sent unmodified.

Bob, on receiving the message, reverse the base-64 encoding and decrypts the IDEA key using his private RSA key, D_B. This IDEA key is then used to decrypt P'.zip. After decompression, Bob separates the plaintext from the encrypted hash, decrypts the hash with Alice's public key, and verifies the integrity of the hash. If the plaintext is in agreement with his MD5 computation, it confirms that the message was correct and was sent by Alice. PGP provides the user with several RSA key size options, depending on the desired level of confidentiality:

- Casual (384 bits): known to be breakable, but with much effort.
- Commercial (512 bits): possibly breakable by three-letter organizations.
- Military (1024 bits): generally believed to be unbreakable

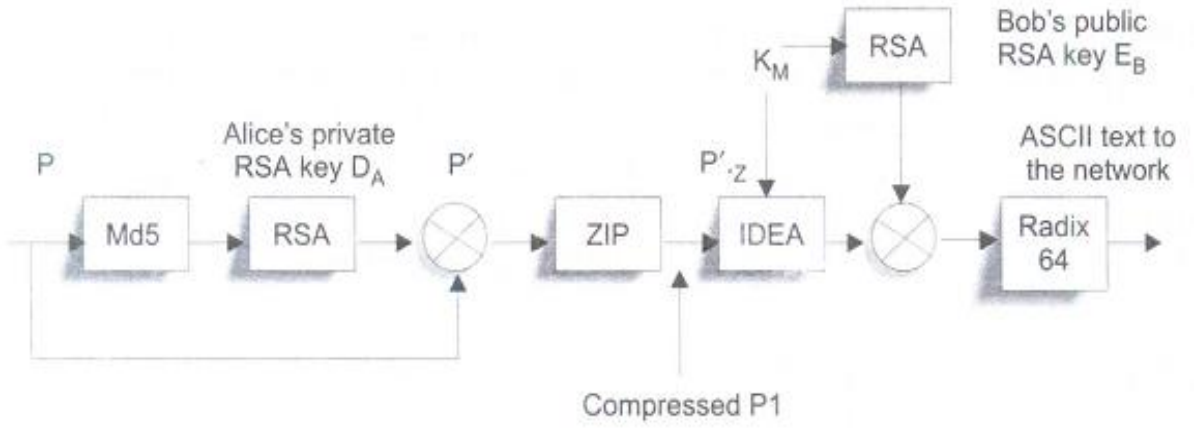


Fig 8.13 Use of PGP in Encrypting a Message

PEM

Privacy Enhanced Mail is a draft internet standard that provides security related services for electronic mail applications. Its most common use is in conjunction with the internet standard Simple Mail Transfer Protocol (SMTP), but can be used with any electronic mail scheme.

The PEM specification consists of the following four RFCs:

a. RFC 1421: Message Encryption and Authentication Procedures
b. RFC 1422: Certificate Based Key Management

c. RFC 1423: Algorithms, Modes and Identifiers
d. RFC 1424: Key Certification and Related Services

PEM is an end-to-end service that is transparent to intermediate mail forwarding elements. The underlying mail system need not be altered to accommodate PEM. It provides protection in SMTP as well as other mail transport environments. PEM also supports the use of advance manual distribution of keys, centralized key distribution based on symmetric encryption and the use of public key certificates. This requires the communicating end systems to share the same key distribution mechanism.

Specifically, PEM provides the following capabilities:

- Disclosure protection
- Originator authenticity
- Message integrity
- Non-repudiation of origin

Messages sent using PEM is first converted to a canonical form, so that they have the same conventions about white spaces (tabs, trailing spaces etc.), use of carriage returns and line feeds. This transformation ensures that message transfer agents are unable to modify the contents. A hash message is then computed using MD2 or MOS. The combination of the hash and the message is encrypted using DES. The output is then delivered to the recipient. Each message is encrypted with a one-time key, which is enclosed along with the message. At the receiving end, the reverse process for decryption takes place.

On the other hand the PEM does not address security related concerns such as access control, confidentiality of traffic flow, routing control, issues relating to the serial reuse of PCs by multiple users, assurance of message receipt, detection of duplicate messages and prevention from replay attacks.

MULTIPLE CHOICE QUESTIONS

Questions for Application Level

a. Ca you tell, Unusual attempt to gain access to a system, or to discover information about the system is called as

A. Probe
B. Scan
C. Account compromise
D. Packet sniffer

b. Can you tell, Large number of probes are called as

A. Probe
B. Scan
C. Account compromise
D. Packet sniffer

c. Can you tell, Unauthorized use of a computer account by someone other than the account owner is defined to be_____

A. Account compromise
B. Packet sniffer
C. Root compromise
D. Exploitation of trust

d. Which of the following Program captures data from packets as they travel over the network

A. Packet sniffer
B. Exploitation of Trust
C. Denial of services
D. Malicious code

e. Which among the following is Generic term for programs that cause undesired results on a system when executed

A. Packet sniffer
B. Exploitation of Trust
C. Denial of services
D. Malicious code

f. Can you tell, Preventing legitimate users from using a service is called as

A. Denial of services
B. Root compromise
C. Account compromise
D. Exploitation of trust

g. Which among the following is Self-replicating programs that spread without any human

intervention, after they are started

A. Trojan
B. Worms
C. Virus
D. Malware

h. What is the Full form of VPN

A. Virtual Private Network
B. Viral Private Network
C. Virtual Public Network
D. Viral Public Network

i. Do you know which is avoidance of the unauthorized disclosure of information

A. Integrity
B. Confidentiality
C. Availability
D. Reliability

j. Do you know which is the computation of a function that maps the contents of a file to a numerical value?

A. Checksums
B. Cryptography
C. Confidentiality
D. Integrity

k. Can you tell how the denial of a commitment is or data receipt is defined as_____.

A. **Repudiation**
B. Denial of service
C. Probe
D. Disclosure

l. What is the discovery of the pattern of traffic between parties called as

A. Disclosure
B. Traffic analysis
C. Masquerade
D. Repudiation

m. Which of the following checks for Information alteration during its transmission over the network?

A. Authentication
B. Integrity
C. Confidentiality
D. Authorization

n. Do you know which among the following is the conversion of electronic data into another form, which cannot be understood by anyone except authorized parties?

A. Cipher text
B. Simple text
C. Password text
D. Encrypted text

o. Can you tell the Full form of PEM

A. Privacy Enhanced Mail
B. Privacy Enhanced Message
C. Public Enhanced Mail
D. Public Enhanced Message

p. Which among the following represents Fixed length groups of bits

A. Blocks
B. Group
C. Clusters
D. Set

q. Can you tell, the interception of information intended for someone else during its transmission over a communication channel is called as what?

A. Eavesdropping
B. Alteration
C. Masquerading
D. Repudiation

r. Can you tell Unauthorized modification of information can be called as which among the following

A. Eavesdropping
B. Alteration
C. Masquerading
D. Repudiation

s. The fabrication of information that is purported to be from someone who is not actually the author is termed as_____

A. Eavesdropping
B. Alteration
C. Masquerading
D. Repudiation

t. Do you know Conventional encryption is also called as _____

A. **Symmetric**
B. Asymmetric
C. Two-way encryption

D. Public key encryption

u. Can you tell Synonym of Asymmetric Encryption is _____
   A. Shared key
   B. Conventional encryption
   C. Public key encryption
   D. Complex key encryption

v. Which of the following RFC is used for message encryption and authentication procedures?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

w. Which of the following RFC is used for certificate based key management?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

x. Which of the following RFC is used for Algorithms, modes, identifiers?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

y. Which of the following RFC is used for Key certification and related services?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

LONG ANSWERS

SKILL

1. Find the different types of Security breaches.
2. What is DOS? Can you see the possible solution where denial of service can be prevented?
3. Find the different goals of Security
4. Find the different threats and attacks possible.
5. What is Sniffing? Can you see the possible solution on how Sniffing can be prevented?

6. Find the different types of network transaction security issues?
7. Find what Cyber security is, and what are its type?
8. Explain the symmetric key cryptosystem with a neat diagram.
9. Explain the public key cryptosystem with a neat diagram.
10. Determine the principle of cryptography and define cipher-text.
11. Find how the secret key signature key works and define digital signature.
12. Find the mechanism of PGP working.

UNIT – V

ELECTRONIC PAYMENT SYSTEM

8.1 INTRODUCTION TO PAYMENT SYSTEM

With the growth of the internet economy, a variety of transactions, some of extremely low value, while others of high value need to be handled. Based on the size of payment, all payment transactions can be classified in the following three categories:

a. **Micro Payments:** These transactions usually involve ones that have very low payment value. At times, the value of a transaction may be a fraction of a currency unit. Typically, transactions that are of five or lesser currency units, in case of dollars and fifty in case of the rupee, are treated as micro payments. Since, the transactions are of such a low value, even a small overhead or a minimum overhead may become unbearable. Thus, systems for micro payments have to ensure near zero overhead in order to make them viable.

b. **Consumer Payments:** These payments typically involve values of five to five hundred currency units, in the case of dollars and euros, and may be 50-5000 units, in case of the rupee. These are the dominant form of payment transactions, as most of the consumers buying in a single shopping trip fall under this category.

c. **Business Payments:** Usually transactions that are of higher amounts-five hundred and above in case of dollars or five thousands and above in case of rupee-are treated as business payments. Businesses payments usually have an invoice associated with them. Business-to-Business payment transactions are in the higher range, and fall in this category.

8.2 ONLINE PAYMENT SYSTEMS

Various methods have been used for online payments. In general, the various payment mechanisms can be broadly classified in to three categories – E-Cash, Cheques and Credit cards. Many virtual shops on the internet accept payment through digital cash, electronic cheques or the credit card mechanism. Digital cash is the electronic equivalent of physical cash, with all the inherent properties of cash embedded in it. Digital cash represents, in a sequence of binary numbers, an intrinsic value in a chosen currency. As the payment systems involve direct financial transaction, dealing with the movement of actual money, they become prime targets for defrauders all over the world. During transmission from the buyer to the seller, the binary numbers are susceptible to interception by packet sniffing programs and hence resultant fraud. Thus, the issue of ensuring integrity, confidentiality and non-refutability acquire an added significance. Encryption offers solutions to some of these problems.

In the real world, we have three distinct types of payment systems - Pre paid, Instant-raid and Post-paid. On the electronic payment front too, payment systems that have evolved can be placed in the above three categories. None of the electronic payment systems are as of now

equivalent to or carry the Government/ Central Bank guarantee, like physical cash; debit cards come closest to instant-paid electronic payment systems.

8.3 PRE-PAID ELECTRONIC PAYMENT SYSTEMS

eCash

eCash is a purely software based, anonymous, untraceable, online token payment system available on Unix, Windows, as well as Macintosh platforms eCash attempts to replace paper cash as the principal payment vehicle in online payments. It combines computerized convenience with security and privacy that improve on paper cash eCash can be held and used by anyone, even those without a bank account. eCash allows for bi-directional payments. There is no distinction between customers and merchants with regards to payments. Both sides can give and receive payments. However, since the system is coin or currency based, it requires clearing of coins by its issuing bank. The implementations of various transactions with eCash are as follows:

- **Withdrawal:** There are two participants in the withdrawal transaction, the bank and the customer. A customer connects to an eCash issuer and purchases electronic coins of the required value. These coins are generated, involving the blind signature scheme to make the tokens anonymous. The customer generates the token ids, blinds them, determines their denominations, transmits them to the issuer that blind signs them and returns them to the customer, who in turn unblinds them and stores them on his PC, in a wallet. No physical coins are involved in the actual system; the messages include strings of digits and each string corresponds to a different digital coin, with each coin having a denomination or value. The wallet of digital coins is managed automatically by the customer's eCash software. It decides which denominations to withdraw and which to spend in particular payments.
- **Purchase:** Once a customer has some eCash on his hard drive, he can buy things from the merchant's shop. If the customer shows the intent to purchase a product, he receives a payment request from the merchant, which he has to confirm. His eCash software chooses coins with the desired total value from the wallet on his hard disk. It then removes these coins and sends them over the network, to the merchant's shop. When it receives the coins, the merchant's software automatically sends them on to the bank and waits for acceptance before sending the goods to the customer, along with a receipt. To ensure that each coin is used only once, the bank records the serial number of each coin in its spent-coin database. If the coin serial number is already recorded, the bank detects that someone is trying to spend the coin more than once and informs the merchant or else the bank stores it and informs the merchant that the coin is valid and the deposit is accepted.
- **Customer-to-Customer:** When a customer receives a payment, the process would be the same. The only difference between payment from a customer to another customer and the earlier one is what happens after the bank accepts the cash. Once the second consumer has configured his software, he requests the bank to withdraw the eCash just deposited, and send it back to his PC as soon as the coins are accepted.
- **Privacy Protection (Blind Signature):** In a simple withdrawal the bank creates unique

blank digital coins, validates them with its special digital stamp and supplies them to the customer. This would normally allow the bank to recognize the particular coins when they are later accepted in a payment and also tells exactly which payments were made by the customer.

- **Security:** By using 'blind signatures', the bank is able to validate coins without tracing them to a particular account. Instead of the bank creating a blank coin, the customer's computer creates the coin itself at random. Then it hides the coin in a special digital envelope and sends it off to the bank. The blind signature mechanism lets the validating signature be applied through the envelope. But the bank cannot tell who made the payment. When the customer's computer removes the envelope, it has obtained a coin validated by the bank's stamp. When he spends the coin, the bank must honor it and accept it as a valid payment because of the stamp.

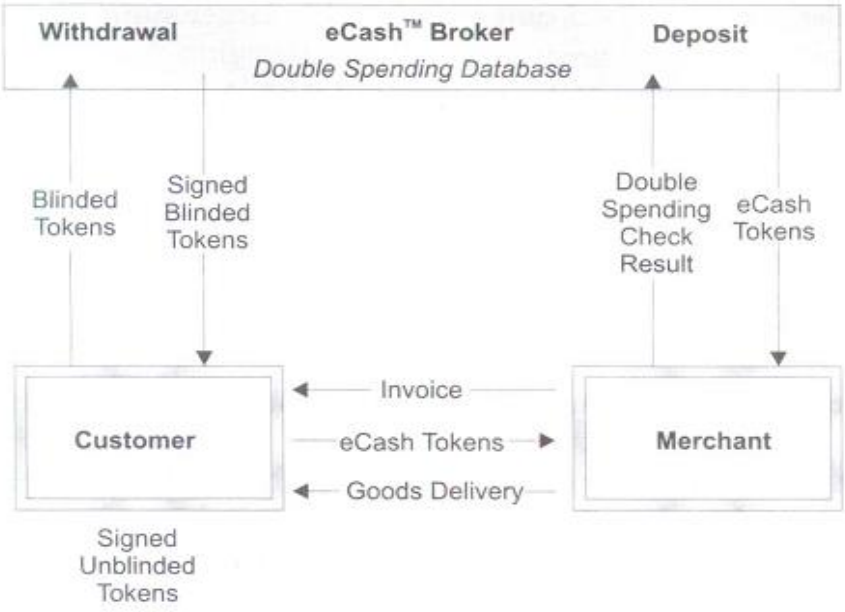


Fig 8.1 Transaction Flow in eCash System

Mondex (E-Wallet)

The Mondex purse or eWallet is a **smart card** alternative to cash. The Mondex purse, a self-standing value store, requires no remote approval of individual transactions. Rather, the mondex value equivalent to cash is stored in the card's microchip. The purse also stores secure programs for manipulating that value and for interfacing with other Mondex cards or terminals. After withdrawal from an ATM, the value (money) can be transferred from one card to another via a special, password protected, electronic wallet. The first implementation of Mondex supports upto five different currencies, each separately accounted for by the card.

The Mondex system uses the following hardware:

- Mondex smart card
- Mondex retailer terminal: to transfer funds from the customer card to merchant

terminal.

- Mondex wallet: a pocket sized unit to for storing larger sums of digital money than the card.
- Mondex balance reader: a small device to reveal the balance remaining on the Mondex Card.
- Mondex hotline: to access the bank account, to transfer money to the card, to check the balance, and to transfer money to other cardholders.
- Mondex ATM: to recharge cards or to transfer money back into the account.

- **Transaction:**

The sequence of steps in a particular transaction is:

1. Customer loads value (money) onto the card either from an ATM machine or from a phone.
2. On purchase of an item, the customer provides his card to the merchant's point of sale device and authorizes the transfer of a certain value.
3. The amount is electronically deducted from the chip inside the customer's card and added to the amount on the retailer's chip.

All this is accomplished without accessing the customer's bank balance or checking his or her credit worthiness.

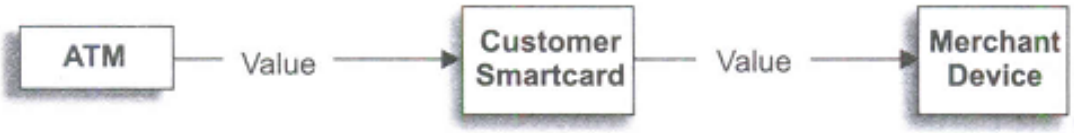


Fig 8.2 Transaction flow in Mondex System

For use over the internet, a Mondex compatible card reader will be attached to the computer. When a transaction takes place, computer talks to the card through an interface. An electronic handheld device lets cardholders check their balances.

- **Security:**

Just like cash, if a smart card is lost or stolen, the cardholder loses real money. However, the Mondex card has a unique feature that allows cardholders to lock the value on the card with a four digit personal number, thereby safeguarding the value held on the card. The system uses special purpose hardware on smart cards to ensure its cryptographic security. An important point about Mondex transactions is that value can only move from one Mondex card to another and can only be stored on Mondex cards.

NetBill

NetBill has been conceived to address the problem of buying information goods over the internet. As opposed to the physical goods purchased on the internet, and shipped later by the merchant, the information goods are themselves transferred over the internet, to the customer. Preferably, this transfer should take place immediately after purchase. Hence, the issues to be addressed in such a transaction are very different from these on transactions involving physical goods.

- **Transaction:**

The transaction flow is depicted in Fig. 8.4 and the sequence of transactions using NetBill is described as follows:

- The customer buys information goods from the merchant.
- The Merchant sends goods, in encrypted form, to the customer.
- The customer software verifies that the goods were received correctly & sends verification of this to the merchant software.
- The merchant submits the verification message received from customer, the account information provided by customer and the decryption key to the NetBill server.
- The NetBill server verifies that the customer has sufficient money in the account to pay for the goods. In case of sufficient funds, it transfers funds, stores the decryption key and sends the report to the merchant software.
- The merchant then sends the customer decryption key, which the software on the customer machine uses to decrypt the goods. In case the merchant server fails to deliver the decryption key, the software on customer server can acquire the key from the NetBill server.

The NetBill server keeps accounts for all merchants and customers. The accounts are linked to accounts at a traditional bank. The NetBill server operates transitionally, to ensure that the consumer does not get billed for goods he cannot decrypt or receive goods without paying for them.

Fig 8.3 Transaction Flow in NetBill System

- **Security:**

NetBill uses a combination of public key cryptography and symmetric key cryptography to make sure that all NetBill communications are secure and all transactions are authorized. NetBill's approach is based on the well tested Kerberos protocol, which is a network authentication system for that allows entities communicating over networks to prove their identity to each other, while preventing eavesdropping. It also provides for data stream integrity (detection of modification) and secrecy (preventing unauthorized reading) using cryptography systems such as DES (Data Encryption Standard).

8.4 REQUIREMENT METRICS OF A PAYMENT SYSTEM

1. Transaction

Transaction, in the context of payment systems, refers to the actual exchange of currency with the goods or documents being transferred. Every transaction should exhibit the following characteristics.

- **Atomicity:** It refers to the system's ability to ensure that no partial transactions or exchanges can take place. In other words, if system failure takes place in the middle of a transaction, the effect of the transaction will be fully erased and system will be restored to the original state. That is, either a transaction should occur completely or it should not occur at all.
- **Transfer of Funds:** There should not be any currency loss in the transaction. Either a full transfer, in which the account of the payer is debited and the account of the payee credited with the corresponding amount-should take place or no change of accounts should occur at all.
- **Complete Transfer:** This is applicable in the case of digital goods transfers over the net. A complete exchange of currency with the corresponding digital goods should take place. If a digital goods delivery is linked to its payment, then either both should happen or none at all. This is also referred to as the fair exchange protocol.
- **Consistency:** There should be no ambiguity in the transaction. All parties concerned must agree on the relevant facts, i.e., amount and reason of transfer, of the transaction.
- **Isolation:** Transactions must be independent of each other. The result of a set of concurrent transactions must be equivalent to a sequential arrangement of these transactions.
- **Durability:** Durability becomes important in case the system crashes during the transfer. Even after a system crashes, the system should recover to a state, where transactions and status information is consistent. If the crash occurred prior to transfer than the system should reflect the prior state, otherwise it should show the durable effect of the transfer.

2. Security

Security, in the context of payment systems, refers to the system's ability to protect all parties from frauds, due to interception of online transmission and storage. The payment system should be secure enough to offer the following:

- **Fraud Protection:** Digital payment systems must be tamper resistant and should have built-in mechanisms to prevent illegal use of digital cash. It must also provide the means for detection and punishment of misuse, after the fraud.
- **No Double Spending:** Since digital cash is represented by bytes that can be easily copied and re-spent, the digital payment system should safeguard against reuse of currency.
- **No Counterfeiting:** The system should be able to detect fake currency. It should be easy to distinguish between legal money tokens and unauthorized illegal money.
- **No Overspending:** The system should have the means to ensure that the user is unable to spend beyond the money represented by token, or held in the purse.
- **Non-refutability:** The parties involved should be able to verify that the payment transaction has taken place, along with the amount and the purpose of transaction
- **Hardware Tamper Resistance:** Some digital payment systems rely on tamper resistant hardware like smart cards to prevent double spending and forgery, and can be used offline.
- **Unauthorized Use:** The tokens stored in soft format/ digital data are easy to steal, a good payment system should prevent the stealer from being able to spend the tokens.
- **Privacy Control:** The payment system should make it possible for customers to keep their spending habits private from observers, merchants, and banks.
- **Confidentiality:** The grants of confidentiality by the payment system are essential to the user. In an ideal situation, the payment transaction should be carried out in such a manner that it maintains confidentiality of all the intermediate information and yet ensures the value transfer.
- **Non-traceability:** Payment systems should ensure ruling out any possibility of two different payments, by the same user, being linked together. The transaction should also maintain anonymity and non-traceability, similar to cash payments in a shop.

3. Interoperability

The interoperability of the payment systems refers to its ability to operate in multiple online as well as offline payment environments. The various issues involved under interoperability are:

- **Divisibility:** Money should allow for both low value and high value transactions. Hence, it should be possible for users to replace a single high denomination transaction by several low denomination transactions as and when desired.
- **Bi-directionality:** The payment system should not only allow the regular merchants to receive payments, but also customers to receive refunds. The payment instrument

should work both ways, without either party being required to attain registered merchant status.

- **Re-spendibility:** The receiver or the owner, of digital money should be able to transfer it to any other person as in the case of normal cash, without the intervention of a third party.
- **Acceptability:** In interest of long term viability, the payment system should not be restricted to any particular financial institution. All institutions and banks should also accept the electronic cash issued by an institution.
- **Multi-currency Support:** Since electronic commerce has a global reach, a single national currency support impedes worldwide acceptance. Hence, the payment system should support multiple currencies and a reasonable mechanism for converting one currency into another. Of course, this requirement is not very easy to implement, given the volatility in exchange rates and limited/restricted convertibility of many currencies around the world.
- **Exchangeability:** It should be possible for electronic payments of one digital payment system to be exchanged for payments of another digital payment system, or for any other bankable instrument.
- **Portability:** Security and usability of a payment system should not be dependent on a certain physical location, e.g., on a particular computer. The owner of the digital currency should be able to spend it from any location, even when on move.

4. Scalability

Scalability refers to the level of operations possible within a certain payment system. The payment systems should be able to support many consumers buying goods at the same time from many merchants, even under peak conditions. The service should be scalable for the load performance, and efficient for the micro payments as well as general payments.

- **Offline Operation:** Usually, the payment systems involve a trusted third party who is online for validation and authorization. It should also support offline operations where the third party is not necessarily available online all the times. This reduces delays and increases availability of the payment system.
- **Micro Payments:** Micro payments refer to payments for services that are offered even at fractions of the basic unit of currency. These services are normally are made available on a pay per use basis. A payment system should make low value transactions economically feasible. Therefore micropayment techniques need to be both inexpensive and fast.
- **Low Costs:** The cost of executing a payment transaction should be low enough to render low value transactions economical.
- **Efficiency:** Digital payment systems must be able to perform micro payments without noticeable loss of performance.
- **Macro Payment:** These payments refer to transactions that usually start from multiple units of the basic currency unit. The system should be able to handle these payments in a secure and efficient fashion.

5. Economy Issues

In order to become an accepted economical instrument, a digital payment system needs to provide a trusted, reliable and economically feasible service to a sufficiently large user community.

- **Operational:** A system should be deployable immediately, i.e., the testing of the payment system should not be so protracted as to render the mass use impossible.
- **Large User Base:** The payment system should be used by a large number of customers. The size of customer base using the digital payment system affects the merchant's attraction to it, while currency acceptance by large number of merchants affects the size of user base.
- **Low Risk:** The electronic payment system should minimize the risk of financial loss associated with the use of such payments systems. It should at best be limited and controlled. To develop trust, users should be protected from financial losses by system misuse.
- **Reliability:** An electronic payment system must be highly reliable in its operation. It should ensure high availability as a temporary failure can cause uncontrollable losses to its user base.
- **Conservation:** It refers to the conservation of value stored in digital currency, over a period of time. It should be easy to store and retrieve the value. The value of money should be lasting in nature, it should diminish when spent, rather than become invalid with the passage of time.
- **Ease of Integration:** The electronic payment system should be easily integratable with applications that conduct the electronic commerce process over the network.

MOBILE COMMERCE - INTRODUCTION, FRAMEWORK & MODELS

9.1 INTRODUCTION

The term Mobile Commerce or M-Commerce has been used to describe a variety of transactions conducted through mobile devices connected through the wireless network. Wireless networks like GSM, GPRS, TDMA, CDMA, and UMTS enable the mobile device user to access variety information stored on databases on connectivity providers, other service providers, and information providers, including information stored on web servers. Here, mobile devices refer to all such devices that connect to wireless networks and are capable of accessing, interacting, answering and displaying the information on the screen. The term mobile device is used here to refer to devices like: Cellular phones, Hand-held computers such as palmtops, tablets PCs and PDAs or Messaging/pager devices.

Mobile Commerce can be defined as any electronic commerce activity conducted over the wireless network through mobile devices. It is the exchange of information, goods, and services through the use of mobile technology.

The different activities that can be performed using M-Commerce are as follows:

- Paying for and downloading ring tones, mp3 music, news or information services
- Receiving parking meter expiry, alerts on handheld devices and paying for additional parking time
- Enquiring the airlines, train or dynamic bus arrival schedules
- Enquiry, reservation and purchase of airlines tickets through mobile wireless devices
- Enquiring about stock market conditions and placing a stock purchase or sales order through the mobile devices
- Receiving the location-specific information regarding restaurants, entertainment complexes through mobile device
- Receiving location-specific advertisement and product discount coupons in the current neighborhood

9.2 BENEFITS OF MOBILE COMMERCE

- Since the consumer using the handheld device comes through a specific wireless network through which the location can be identified. The location identifiable connectivity offered by mobile commerce not only enhances the benefits made available by the electronic commerce but additionally helps in providing more relevant content.
- The round the clock (24x7) availability offered by the Internet is also available to mobile commerce users, anytime & anyplace. This benefited many users of electronic commerce as they could conduct their business and access information at convenient times and from the confines of their homes or any other place, provided it had internet connectivity.

- A mobile user trying to locate an ATM teller can contact the banking service provider which in turn can download the location of the nearby ATM center.
- Mobile commerce offers a greater deal of flexibility in accessing the information through a personalized mobile environment.
- Timely information such as flight availability and flight schedules can be obtained even at the last minute.
- The last minute on-the-move access offered by mobile commerce extends electronic markets further as the last minute availability information often leads to immediate purchase.
- Mobile devices, as they remain connected all the time and in possession of the user, can also be used for delivering time critical as well as emergency information.
- SMS based notification and alert services can be put to use to inform users of changes in flight schedules, stock prices, etc.
- The very nature of wireless infrastructure assists in identifying mobile users in certain specified geographic regions. Thus, region specific promotion or information distribution can be easily accomplished in the mobile commerce environment.
- Mobile commerce offers better opportunity for personalization of information and delivery of content that is relevant to the mobile user.
- If the user requests information regarding certain products, the advertiser can deliver the information about the stores that stock the targeted products. In other words, mobile commerce offers advertisers an opportunity to deliver time sensitive, geographical region specific information along with promotional discount coupons anytime, anywhere.
- Electronic commerce payment models require third party mechanisms such as credit cards. Mobile commerce, on the other hand, can utilize the mobile device itself for payment purposes and payments made on the device can appear as part of the phone bills. Users can thus pay for parking meters, taxis, petrol, etc. through the mobile device.

9.3 IMPEDIMENTS (ISSUES) IN MOBILE COMMERCE

- **Mobile Screen Resolutions:** Mobile handheld devices commonly used today include phones and palm-sized computers. The very nature and purpose of these devices offers a limited screen size. In web browsing users can get a rich experience of browsing the product details on 800x 600 pixel sized screens with rich colors and a tool set to offer 3-D and even video experience.
- **User Interface:** The graphic user interface of the web browser offers the point and click interface. Although, handheld devices provide a great deal of flexibility and mobility in accessing the information, they have far lesser convenient user interface when compared to personal computers. In contrast, mobile devices offer menu based scroll and click interface. The physical lightness and small-size of the device poses limitations in the development of convenient input and display interfaces.

- **Memory:** Mobile devices also have limited computing power and memory and storage capacity. As a result, they are unable to run and support complex applications.
- **Incompatible Networks:** The cellular networks evolution in the past decade has created multiple competing protocol standards. In the United States much of the mobile networks deployed have been using Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). On the other hand, many European nations and the Asia-Pacific region adopted the General System for Mobile Communication (GSM). Later in India, most of the cellular phone operators adopted the Reliance Info Com., which used CDMA for wireless networks. Although the interconnect arrangements do exist between the multiple players, yet mobile commerce application builders have to be aware of the heterogeneity of the network protocols and ensure that the application is able to operate seamlessly in any network.
- **Bandwidth Access:** Wireless networks use frequency spectrum for exchanging information. In order to promote healthy competition amongst wireless operators and judicious use of limited spectrum, regulatory bodies control the spectrum. In India, frequency spectrums were initially allocated and regulated by the Department of Telecommunication (DoT). The Telecom Regulatory Authority of India (TRAI) was later set up to manage the spectrum.
- **Security Concerns:** Mobile commerce operates over wireless networks making it more vulnerable to intruders compared to wired infrastructure. In the wired network, the intruder has to gain physical access to the wired infrastructure while in the wireless network the intruder can be anyone with the ability to receive signals on his wireless intrusion device. Also, from the technology standpoint, the wireless infrastructure is faced with the following security related concerns.
    - Since handheld devices have limited computing power, memory and storage capacity, it is difficult to deploy encryption schemes without severe degradation in performance.
    - The atmospheric interference and fading of signal in wireless channels causes frequent data errors and sometimes even disconnection. A disconnection in middle of a financial transaction can leave the user unsure and distrustful and may also lead to vulnerability.
    - Authentication of mobile devices prior to carrying out any transaction is a major issue. The network is capable of authenticating the SIM, but a SIM user cannot authenticate the network. Therefore, a sound commerce environment requires that both sides should be able to authenticate each other.
    - The disconnection and hand-off issues pose additional problems in trying to maintain the identity of the mobile device and authentication of it being in order.
    - The encryption mechanism may make it harder to decipher but inability to use higher key lengths for encryptions increases the degree of vulnerability.
- **Competing Web Language:** Mobile devices cannot handle full-fledged Hyper Text Markup Language (HTML) documents. In order to offer web access and offer similar services, two competing but incompatible standards have emerged. The mobile devices that adopt Wireless Access Protocol use Wireless Markup Language

(WML) for mobile commerce applications, while the NTT DoCoMO's iMode devices use a condensed version HTML (CHTML). In order to enable voice access and interface for displaying web content, VoiceXML, a new markup language, has also emerged. Incompatible standards make the task of mobile commerce application and service providers even more complex.

9.4 MOBILE COMMERCE FRAMEWORK

Mobile commerce applications require a reliable wireless **network infrastructure** to move the information and execute transaction in a distributed environment. These applications also rely upon two key component technologies, i.e., the **information publishing technology** necessary for the creation of suitable digital content that can be browsed through handheld devices with limited memory, storage, and processing capabilities; and information distribution technology to move digital contents and transaction information over wireless networks. Thus, in the mobile commerce framework, network infrastructure forms the very foundation while publication and distribution technologies are the two pillars that support the creation of distributed mobile commerce applications. In addition to technological infrastructure and applications, for electronic commerce to flourish it is essential to have a **business service infrastructure**. The business service infrastructure comprises of directory services, location and search services, and trust mechanism for private, secure, reliable and non-repudiable transactions along with online financial settlement mechanism, that operate over the wireless network.

The multi-layered architecture of electronic commerce, comprising of essential blocks has been shown in Fig. 10.1. The framework describes various building blocks enabled by technology for creating new market and market opportunities. The building elements of the mobile commerce architecture are described as follows:

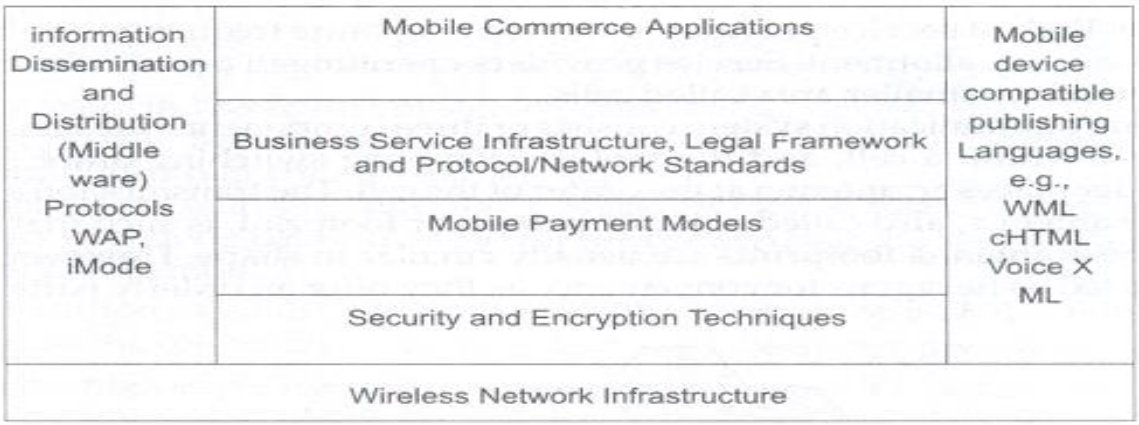


Fig 10.1 Architectural Framework of Mobile Commerce

9.4.1 Wireless Network Infrastructure

This layer is also called as the **Information Superhighway**, as it is used to move and execute the transactions in the mobile commerce environment using dedicated network cables

which may be wired or wireless cables. It is the combination of several technologies such as the availability of digital communication through hand held devices, embedded operating software for processing information and digital connectivity through wireless networks which are essential requirements for mobile commerce applications to operate.

Wireless networks have evolved from the basic voice only radio based analog transmission and have acquired the digital voice and data transmission capability. Wireless networks today are capable of achieving 2 Mbps data rates. The following Table 10.2 describes the evolution of the wireless networks.

This layer is also called as the **Information Superhighway**, as it is used to move and execute the transactions in the mobile commerce environment using dedicated network cables which may be wired or wireless cables. It is the combination of several technologies such as the availability of digital communication through hand held devices, embedded operating software for processing information and digital connectivity through wireless networks which are essential requirements for mobile commerce applications to operate.

Generation	Channels	Swithching Mode	Examples	Data Rates
1 G	Analog Voice	Circuit Switched	AMPS	N/A
2 G	Digital	Circuit Switched	GSM	9.6Kbps
		Packet Switched	CDMA	
2.5 G	Digital	Packet Switched EDGE	GPRS 384Kbps	171.2 Kbps
3 G	Digital	Packet Switched	CDMA2000 WCDMA	

Fig 10.2 Evolution of Mobile Networks

In the cellular mode of communication large geographical regions are identified and allocated to service providers. The Telecom Regulatory Authority of India (**TRAI**) handles the allocation and other regulatory issues, such as how many players can operate within a specific area. Each of service provider is allotted a separate frequency sub-bands within the overall frequency allotment. Service providers operating in a particular region divide the entire region into smaller area called cells.

The cellular communication system consists of three components: the **handheld device**, the **transceiver** within a cell, and the mobile telephone switching office (**MTSO**). The service provider places an antenna at the center of the cell. The transmission and reception pattern of the antenna, also called antenna pattern or footprint, is such that it covers the entire cell.

In a wired internet environment, FTP, HTTP, SMTP and other protocols are used for exchanging multimedia contents consisting of text, graphics, audio and video data, whereas in wireless devices like digital mobile phone, the **Wireless Access Protocol (WAP)** is the most commonly used standard for exchanging multimedia content and information services between wireless mobile devices. **WML** (Wireless Markup Language) is the language used to create

the pages in a WAP browser. WAP is the bridge that assists in developing technology independent access to the internet and telephony services from wireless devices.

9.4.2 Security and Encryption

In the mobile commerce environment, since the information is made available through the WAP gateway or through iMode, the information source security depends upon the security provided by the appropriate gateway protocols. In case of WAP gateways, the Wireless Transport Layer Security (WTLS) implements the information source security to block unauthorized access and modification of information content.

The second issue of securing the transaction carried out between the information server and the mobile user requires addressing of several security and confidentiality related issues that are present in the case of wired electronic commerce as well. Obviously, in order to build trust amongst mobile device users to carry business transactions through the mobile devices in an open, wireless, universally accessible environment, it is important that the security of the transaction is ensured. The three fundamental issues that need to be addressed to create a trustworthy business environment are the following:

1. Authentication
2. Integrity
3. Confidentiality

Encryption techniques such as shared/ symmetric key as well as the public/private key pair based encryption techniques along with the pubic key infrastructure (PKI) supported digital certificates, have been used for addressing transaction security issues in electronic commerce. Mobile commerce operates through wireless devices over broadcast-based radio transmission or other wireless networks. The additional weaknesses, emanating due to the wireless network environment, become a source of attack on transaction security by unwanted intruders.

Authentication: In a mobile environment, during the transaction itself the mobile device user may change its location, resulting in change of IP address; in case of an IP based network or handling base station identity change may be in case of phone-based connections. In case of the phone-based connection, the mobile user location change in addition to resulting, in handling base-station identity change, may also result in loss of connection as the use may move out of the coverage area. Thus, authentication in the mobile commerce requires more involved protocols that address the issues raised here.

The Wi-Pi Protection Access (WPA) Security specification has been developed for mobile commerce systems and gradually many networks have adopted it. The WPA specification describes the protocol for user authentication. There are several extensible authentication protocols (EAP) such as Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) for mobile networks,

which prevent unauthenticated or unauthorized access and rogue access point creation in the wireless network.

Integrity and Reliability: The fading of the signal in a radio-based transmission and interference from the other transmission sources and noise are common phenomenon. In the wireless environment, the content of the message may often be lost due to the above phenomenon. Thus, the integrity of the message may be lost quite frequently due to intended as in case of active intruder or through the interference and unreliability of the transmission network. The mobile nature of the device will lead to frequent location changes of the client, due to which often messages may arrive from different locations; the problem may further be compounded due to dropped calls. In a wired network users have come to rely on the consistency of their transactions, that is, once the transaction is committed its impact will be complete and final and in case of abortion, or partially computation, and transaction abandonment, the impact will not be seen. In case of dropped calls, the mobile user is left in lurch about the status of the transaction as he/she may not know the commitment status of the transaction. The call hand-offs from one handling station to another also may lead to unreliable states at times. The mobile commerce environment had to address these issues as well in order to establish a trustworthy business environment. The Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) protocols have been developed for ensuring integrity and validation of data.

Confidentiality: Wireless networks transmit radio signal through the air, making it possible for anyone and everyone to access, record, or intercept them. Thus, any message transmitted in the clear can be easily intercepted and interpreted by any intruder. Therefore, encryption of all the transmission is of paramount importance not only for the actual transaction but also for common information exchange in order to ensure privacy. Encryption and decryption is a computation intensive process. Mobile devices have limited computing, processing, and memory power and, thus encryption and decryption of every message puts a demand on already limited resources. Based on the power of the currently available devices, it is not possible to support encryption standards higher than the 256 bits.

9.4.3 Mobile Commerce Payment Systems

Online payment is fundamental to the acceptance of mobile commerce as a viable alternative. It is a mechanism that facilitates an online financial exchange between concerned parties. In the expanded scenario of mobile commerce with geographically dispersed retail buyers and suppliers unknown to each other, mechanisms based upon limited number of well-known participants do not have flexibility to scale-up to the emerging electronic markets. Several scalable and flexible mobile payment mechanisms have emerged, which essentially imitate traditional payment mechanisms, such as cash, checks and credit cards. Electronic payment mechanisms represent currency in the form of digital bits and require the security and encryption mechanism to ensure that the information cannot be duplicated, re-used or counterfeited, yet they need to be freely exchanged.

Some of the factors that are essential of newer payment systems are:

- **Simplicity and Usability:** Obviously, friendly user interface is an important factor in adoption of any service. The availability of a wide range of goods and services, geographical availability of the service and reliable and effective delivery of goods are other important factors that make a payment system usable and simple. The low barrier to learning and adoption of payment system and ease of use/ convenience to the consumer, personalization of the service makes it possible to integrate any system in to daily payment activities.
- **Universality:** A single integrated platform of payment service that can satisfy the need any systems in of person-to-person (P2P), business-to-consumer (B2C), and business-to-business (B2B) payments in geographically spread out markets that are domestic, regional and global.
- **Interoperability**: In any financial payment system, the user should be ensured of interoperability amongst the multiple payment systems, as the world is going to remain heterogeneous in nature and many modes of payments may remain in existence. The objective of achieving Interoperability is often conflicting. Standardization and interoperable protocols for interconnection of networks and systems have made this a technically easy and cost-effective problem to be addressed.
- **Security, Trust, and Privacy:** Trust is the most important aspect of any payment system. Anyone adopting mobile payment mechanism is expected to place inherent trust in the system by granting access to personal bank accounts to the software owned and operated by a non-banking company. The trust can be build by technology-based assurance against fraud and other security issues. Unless, users are assured that the mobile payment system follows tried, tested and true secure banking practices, it is unlikely that users will adopt it. The user should also have option to assure the privacy while making payments.
- **Cross-Border Payments:** In the emerging global market place, a good payment system that is likely to find a wider adoption is one in which it is possible to make cross-border payments almost as easily as local payments. The user should be able to make multicurrency cross-border payments irrespective of his own location.
- **Cost Effective:** The mobile payment system should be cost effective compared to the existing payment systems. Since the cost of per payment transaction is dependent on the overheads, infrastructure, and operational cost, the technology and economy of scale are important factors. Also, the cost of fraud is indirectly passed on to the per transaction costs a system that can minimize fraud can also reduce cost.
- **Speed:** Mobile and technology savvy users are looking for speed of transaction. A mobile payment method should decrease transaction time and automate transactions.

Mobile Payment Models

The mobile payment models can be classified in one of the following categories. But, in the long term the successful implementation of a model will be a hybrid of these, which requires the cooperation and coexistence of the main players.

- **Acquirer-Centric Models:** In the acquirer-centric model all the interactions with the mobile devices are handled by the merchant or his/her agent. The models require specific protocols and certain minimum level of capabilities in the mobile devices of the users. The dual chip or dual slot based payment system typically fall in this category.
- **Issuer-Centric Models:** In issuer-centric models the issuer and the customer who is using the mobile device interacts directly or through agents and handles the whole process. The merchant is not concerned about the processes being followed at the issuers end for processing a payment. The existing electronic payment protocols operating on the wired infrastructure are usually deployed for transferring and processing payment from the issuer to the merchant. Essentially, the interaction between the customer and the issuer use the mobile payment mechanism. The customer operating the mobile device drives the interaction processes.
- **Mobile Network Operator Centric:** Mobile network operators have the billing system to manage customers' phone accounts with them. The billing systems of mobile network operators had been designed for billing mobiles services such as calls and messaging services, utilized by the subscribers. With the introduction of data services where the content may be offered by the third party, billing systems of mobile network operators have become more sophisticated to in order to take care of billings related to the data services utilization and collection of the payment for third party services, in case the third party content was being offered as an integrated service by the mobile network operator. Thus, the pre-paid mechanism can be extended to deduct the charges for integrated and partner third party services, in addition to the call related services of the mobile network operator.

Therefore, in the mobile network operator centric model the mobile network operator performs the billing either on the pre-paid user account or through the phone bill for their postpaid users. Revenue-sharing arrangement among multiple mobile network operators and third party content providers are becoming common in order to broaden the their customer base.

9.4.4 Infrastructure, Legal framework and Network/Protocol Standards

Earlier access to the ecommerce activities like sales, purchase and auctioning was limited to those users who had the wired internet connection and operated from fixed locations in their houses or offices. The emergence of wireless networks further enhanced the reach of online access and users were able to reach out to the global digital marketplace on internet, while on the move. As mobile telephony began to mature and acquire data transmission and reception capabilities, access to online information was no longer limited to the wireless Internet. As mobile users across the globe have been growing at an astonishing pace, mobile telephony infrastructure came up with 2.5G and 3G capabilities, which provided viable data rates for transactions to be carried out over mobile phone networks.

Digital markets require technology transparency and uniform access across information sources. With the standardization of TCP/IP network protocols like FTP and HTTP along with other related information access, distribution and delivery protocols, electronic commerce was able to address infrastructural issues. Various competing mobile network operators have built the infrastructure around competing technologies. Even within the infrastructure of the single mobile operator several generations of technologies may exist. Thus the mobile commerce requires standard mechanism or protocols that make seamless access across technologies and generations possible. Standards and protocols, such as the Wireless Access Protocol and i-Mode, have addressed the gap in this area. The wider adoption of interoperable standards is needed for making mobile commerce a barrier-less marketplace.

In addition to the standards for network and information access and distribution protocols, the technology framework for offering secure, authenticated transaction and its legal protection, and an open competitive market for mobile network access is important for the growth of the marketplace. Under the current policy guided by the Telecom Regulatory Authority, today an Indian consumer has the choice of opting for a multiple mobile connectivity through at least 4 mobile network operators in a single zone. Several major mobile network operators have established networks nationwide, namely, BSNL, Bharati, BPL, Airtel, TATA Telecom, Reliance and HFCL, who have become prominent players in the mobile network operations.

To provide the legal framework to electronic commerce transactions, the General Assembly of the United Nations adopted a Model Law on Electronic Commerce in 1997. The Information Technology Act 2000, based on the Model Law, forms the legal framework of electronic commerce in India. The IT Act 2000 provides for the office of Controller of Certification Authorities (CCA) responsible for setting up the Public Key Infrastructure (PKI) in India through certifying authorities. The IT Act defines the concept of an electronic record as that which can be used as a substitute for paper records. The emergence of mobile commerce has given rise to several issues related to the nature of transactions conducted over the wireless network, mainly due to computing capabilities available in the client (handheld) devices. Several important lighter weight, card-based authentication mechanisms have been proposed and deployed in the mobile commerce arena. This means that the IT ACT 2000 may require certain modifications to expand its scope to include some of these new emerging technologies.

Finally, as of today most of elements described in the framework are in operation, but are still evolving with advances in the technology and business requirements. As a result, the mobile commerce applications for conducting business to consumer (B2C) and business to business (B2B) transactions have evolved. These businesses have been based on various business models, some transplanted from the traditional world, others born as a result of technology.

9.4.5 Mobile Commerce Revenue Streams

With the growth in the number of mobile users with data access, several sources of revenue streams have become possible. Some of the important revenue streams that are possible in the mobile commerce value chain are as follows:

1. **Mobile Connect-time Communications -** Subscription to the mobile basic connectivity services, short messaging services, and other add-ons come at a charge. Also, the charges accrue with the extent of usage of the particular service as well.
2. **Mobile Equipment and Device Providers -** Mobile infrastructure builder and equipment providers operating the network and manufacturing handheld devices are major source of revenue generation in the mobile commerce economy. As more and more digital applications grow on the network, the corresponding equipment and device market also becomes sophisticated and grows with more users and traffic coming in.
3. **Value-Added Services -** Subscriptions to specific services such as news headlines, sports score, entertainment related information, downloading of ring-tones, bill payments, stock market ticker information, and notification services are some the services that are often provided through mobile services. These services may themselves come at a charge and they also increase the network traffic, thus increasing the operators' revenue.
4. **Mobile Application Developers** - Early adopters of mobile technology and its applications had to develop their own application services and incurred heavy expenses. Generic mobile applications have appeared in the marketplace as larger numbers of businesses are adopting mobile commerce. IBM, Microsoft and Oracle already provide mobile applications software. Many other applications for the vertical markets have also emerged.
5. **Mobile Commerce Applications Service Providers (MASP)** - The evolution in information technology and wireless networks is quite swift, making it difficult for even best of businesses to keep up with the rapid changes. MASPs are the new intermediaries that quickly enable mobile commerce in these businesses and help them, in keeping up with the evolution. A MASP free corporate clients by hosting their content using its own infrastructure and offers, anytime anywhere access.
6. **Portals -** A portal in this context usually refers to web sites that serve as entry points for accessing the content and services available on the Internet. Portals aggregate a large number of users and content providers. In the context of mobile commerce, a portal is also an entry point that has been optimized for mobile access. A mobile portal, like its counterpart the Internet portals, act as a gateway to content and transaction-based services. It provides services like content creation, content aggregation and content distribution.

9.4.6 Mobile Commerce Applications

As a result of the potential offered by revenue streams several prominent mobile commerce applications have been deployed. Some of these applications are given below:

- **Mobile Advertising**: Advertising has become a major source of revenue for most of

the portals through banners and other search specific targeted advertising capability. Mobile infrastructure and access has grown at a faster pace than the Internet and has created a huge market space for advertisements. The mobile market space displays advertisements not only based on the information available with the wireless service providers but also based on the current location of the user. Thus, an advertisement placed on the mobile devices can be made location-specific. The advertisement can update users about the various activities and discounts available to the user in the surrounding area of the current location of the user.

- **Mobile Auctions:** With the growth of eBay, OLX and Baazee, the popularity of auctions over the internet has already been proven. Mobile devices further increase the reach of electronic auction markets. A user on the move can access specific auction site, make a bid, monitor bids, or even, on set alarm to get an SMS as and when he/ she has been outbid in order to take a timely action on the bidding process.
- **Mobile Entertainment:** Today, mobile devices are capable of playing audio, video, games etc, but are not capable of storing a huge library due to limitations in memory and storage capacity. Businesses using applications that offer entertainment services such as these on a pay-per-event, pay-per-download, or on subscription basis can cater to a vast number of users who carry mobile devices today and are willing to pay for such services. Mobile device users can subscribe to entertainment libraries. Subscribers these libraries can search for songs, video clips, or games and download them in the device memory for playing.
- **Mobile Financial Services:** In addition to accessing banking services, stock market and other financial information from mobile devices, some applications have been developed to make the mobile device suitable for the payment purposes. The micro-payments through mobile devices is the newest application, where the mobile device is able to communicate with automatic dispensing & vending machines using the wireless network in order to purchase an item stocked by the vending machine. Payment is made through the mobile device to the vending machine and on receiving the payment the machine dispenses the product.
- **Location and Search Service:** The Internet increased the market access of customers by making it possible for them to search for a product, service or a person based upon the specifications and attributes that they are looking for. The search of the product, service or a person is global in nature. A consumer interested in buying a digital camera within a certain price range with specifications could locate its website all over the world. Some other consumers may like to collect the information and search the product through the Internet, but would like to visit the show room to experience the product before purchasing it. In all these cases, it is important that the location and search service should be able to point to providers who offer the product or service in the city of the mobile user's current location.

Mobile devices can be also used for getting the directions to restaurants, movie complexes, and other addresses while on the move. The map and directory services offered by Google and Yahoo! between any two points can be delivered to the mobile device itself. The

location of the mobile device provided by wireless network operators can be used as the source location.

Multiple Choice Questions

Understanding

a. What do you think, Poor e-banking planning is connected with _____

A. Strategic Risk

B. Legal Risk

C. Market Risk

D. Customer Risk

b. Can you clarify, the License to issue digital signature certificates are issued by _____

A. Finance Minister

B. Banks

C. Controller

D. User

c. Can you clarify, Key used to create digital signature is _____

A. Public key

B. Private key

C. Linear key

D. Normal key

d. What do you think, For which card one has to make advance payment?

A. Smart card

B. Gold card

C. Debit card

D. Credit card

e. What do you think, Smart cards are based in _____ standards.

A. SET

B. MIME

C. HTTP

D. TULIP

f. What do you think, Digital signature certificated are issued by _____

A. Central government

B. State government

C. Certifying authority

D. User

g. What do you think, The primary type of website used for e-banking is _____

A. Information

B. Transaction

C. Both A and B

D. Normal website

h. Can you tell, PIN in ATM card id of _____

A. 4 alphabets

B. 2 alphabets and 2 digits

C. 4 digits

D. 1 digit

i. Can you tell which one of the following is a safety measures in banking network

A. Router

B. Firewall

C. Modem

D. Switch

j. What is e-sign act?

A. Electronic sign act

B. Electronic signatures in global and national commerce act

C. Electronic signatures in national and global act

D. Electronic act

k. Who can pass the law for e-banking?

A. RBI

B. Merchant association

C. Parliament

D. State government

l. What is the full form of ATM?

A. Automatic Transaction Machine

B. Advanced Teller Machine

C. Automated Teller Machine

D. Accurate Teller Machine

m. Can you tell, Intrusion detection system helps in what?

A. User enrolment

B. Rapid intrusion detection and reaction

C. Training

D. Independent testing

Skill

n. Do you know, Payment gateways are used for what?

A. Interbank

B. Delivery process

C. Purchase

D. Client

o. Do you know, which is used to converts data transmission protocol between network

A. Gateway

B. Switch

C. Hub

D. Router

p. The customer access e-banking services using _____

A. PC

B. PDA

C. ATM

D. All of the above

q. In credit card what is the grace period of payment?

A. 10 - 15 days

B. 5 - 20 days

C. 15 - 45 days

D. 1 - 2 days

r. The most common payment especially for low value purchase, is made by _____

A. Debit card

B. Credit card

C. Cash

D. ATM

s. Transactional e-banking is typically a front end system. That realises on a programming like _____

A. Inter phase

B. Interlink

C. Inter join

D. Internal

t. Do you know, For which card one has to made advanced payments?

A. Credit card

B. Debit card

C. Smart card

D. Gold card

u. Knowing someone else password by certain illegal means is _____

A. Hacking

B. Plagiarism

C. Log on script

D. Password policy

v. Do you know, Loss of trust due to authorized activity on customer account is concerned with _____

A. Reputational risk

B. Liquidity risk

C. Market risk

D. Identity risk

w. The potential hard for informational website e-banking is _____

A. Viewing account

B. Spreading virus

C. Checking balance

D. Making online payment

x. Can you tell, A debit card/ ATM card is a _____ digit numbers.

A. 12

B. 13

C. 16

D. 10

y. Can you tell, Securer electronic transaction is a _____

A. Protocol

B. Transaction type

C. Security agency

D. JSP

Long Answers

Understand

1. Illustrate the different categories of payment systems.
2. Illustrate the different types of prepaid electronic payment systems.

3. Write in your own words the major impediments faced by the mobile commerce environment.
4. Can you write a brief outline about requirement metrics of a payment system.
5. Write in your own words the different activities that can be performed using M-Commerce.
6. Illustrate the factors that are essential for Mobile Commerce payment.

Application

7. Analyse the working of Mondex electronic payment system.
8. Analyse the working of NetBill electronic payment system.
9. What are the important revenue streams in developing business in m-commerce?
10. Analyze the architectural framework of m-commerce with a neat diagram.
11. What are the different application of M-Commerce.
12. Analyze the online payment system concept.

QUESTION BANK

UNIT I

MULTIPLE CHOICE QUESTIONS

Remembering

a. Can you name which phase of E-commerce system has replacement of parts or item?

A. Information Exchange

B. Contract and Order

C. Shipment and Payment

D. Customer Service

b. *Can you name Which perspective says that EC is the application of technology toward the automation of business transactions and work flow.*

A. *Communications Perspective*

B. *Business Process Perspective*

C. *Service Perspective*

D. *Online Perspective*

c. *What is the full form of B2B*

A. *Business to Business*

B. *Bank to Bank*

C. *Bank to business*

D. *Business to Bank*

d. *Can you name Which E-commerce supports Inter-organizational interaction*

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. Consumer-to-Business (C2B)

D. *Consumer-to-Consumer (C2C)*

e. *Can you name Which e-commerce is also called demand collection model?*

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. Consumer-to-Business (C2B)

D. *Consumer-to-Consumer (C2C)*

f. *Can you name Which E-commerce supports Intra-organizational interaction*

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. Consumer-to-Business (C2B)

D. *Business-to-Employee (B2E)*

g. *What is the Full form of VAN*

A. *Value added Network*

B. *Value area Network*

C. *Validation added network*

D. *Validation area network*

h. *Define Electronic Commerce*

A. Commerce of electronic good

B. Commerce which depends on electronics

C. Commerce which is based on the use of internet

D. **Commerce which is based on transactions using computers connected by telecommunication network**

i. What is the Full form of EDI

A. Electronic Data Interchange

B. Electronic Digital Interchange

C. Electronic Data Issue

D. Electronic Digital Issue

j. Can you name, EDI is most commonly used in Which type of E commerce

A. B2B

B. B2C

C. C2C

D. C2B

k. What is the Full form of EFT

A. Electronic Fund Transfer

B. Electronic Faster Transfer

C. Electronic Fund Technology

D. Electronic Fast Technology

l. Can you name under which E-commerce Stock Market comes

A. B2B

B. B2C

C. C2C

D. C2B

m. Can you name which among the following is not part of B2B architectural model

A. Supplier Oriented marketplace

B. Buyer Oriented marketplace

C. Intermediary Oriented marketplace

D. Time Oriented marketplace

Understanding

n. Can you clarify, Banner advertisements are included in _____ phase of E-commerce system.

A. **Information Exchange**

B. Contract and Order

C. Shipment and Payment

D. Customer Service

o. Can you clarify this, EC is the delivery of information, products /services, or payments over the telephone lines, computer networks or any other electronic means, which of the following perspective define this?

A. *Communications Perspective*

B. *Business Process Perspective*

C. *Service Perspective*

D. *Online Perspective*

p. *What do you think, E-bay is an example of which type of E-commerce*

A. *Online Auctions*

B. *Internet Banking*

C. *Online Ticketing*

D. *Electronic Payments*

q. *What do you think, After choosing to visit the web store, the consumer is typically connected to_____*

A. *Online transaction server*

B. *Private Gateway*

C. *Processing network*

D. *Merchants Bank*

r. *Can you clarify, In which process of ecommerce, the labelling of product is done*

A. Places an order

B. Order details are entered into your business software

C. Order is passed to the warehouse to be processed

D. *Processing order for Shipping*

s. *Can you clarify, Which type of Ecommerce focus on consumer dealing with each other.*

A. Business-to-Business (B2B)

B. Business-to-Consumer (B2C)

C. Consumer-to-Consumer (C2C)

D. *Business-to-Employee (B2E)*

t. Can you clarify, Stock availability, item location criteria are mentioned in _____ list

A. Pick List

B. Sample List

C. Product List

D. Payment List

u. What do you think, Which of the following basic system functionalities is used to display goods on a Web site?

A. Shopping cart system

B. Digital Catalog

C. Customer based database system

D. Product database

v. **Can you clarify, Which type of Ecommerce deals with auction?**

A. B2B

B. C2B

C. B2C

D. C2C

w. What do you think, Amazon is a best example of _____ site

A. Blogging

B. Social Networking

C. E-commerce

D. Entertainment

x. What do you think, Which of the following is not an example of eCommerce site?

A. Amazon

B. Flipkart

C. E-bay

D. Twitter

y. What do you think, Most individuals are familiar with which form of E-commerce

A. B2B

B. B2C

C. C2B

D. C2C

Long Answers

Remembering

1. What are the different perspectives of E-Commerce?
2. What are the different applications of Ecommerce?
3. Find the benefits of Ecommerce
4. Identify the Examples of e-Commerce
5. What are the different architectural model in B2B E-commerce
6. With a neat diagram Explain how C 2C E-Commerce functions

Application

1. Differentiate Ecommerce and Traditional Commerce
2. Analyse the different phases of E-market with neat diagram
3. Can you explain the Top-level ecommerce Process Flow with a neat diagram
4. Demonstrate the detailed working of receiving orders with neat diagram

5. Can you explain how the Processing of an Order is done in the Warehouse with neat diagram
6. Demonstrate the Processing of an Order for Shipping is done explain the concept with neat diagram

UNIT II

MCQ

Understanding

a. Can you clarify which of the following describes a set of business entities and interrelationships among them.

A. Business Model

B. Account Model

C. Transaction Model

D. Inventory Model

b. What do you think,_____ provides the broad perspective necessary for identifying appropriate solutions at some level of abstraction

A. Business Model

B. Account Model

C. Transaction Model

D. Inventory Model

c. Can you clarify, which allows the internet users a free download of internet products and applications.

A. Business Model

B. Account Model

C. Transaction Model

D. Freeware Model

d. What do you think the Full form of FTP is?

A. File Transfer Protocol
B. File Transfer Program
C. Fund Transfer Protocol
D. Fund Transfer Program

e. What do you think the Full Form Of MTU is?

A. **Message Transfer Agent**
B. Message Transfer Aid
C. Media Transfer Agent
D. Media Timed Agent

f. Can you clarify, Which field of Email has Blind of carbon copy recipients in it.

A. To
B. From
C. CC
D. BCC

g. Can you clarify, Which field of Email has Short Title of the message
   A. From
   B. Subject
   C. CC
   D. BCC

h. What do you think the Full Form of SMTP is?
   A. Simple Mail Transfer Protocol
   B. Small Mail Transfer Protocol
   C. Sample Mail Transfer Protocol
   D. Switched Mail Transfer Protocol

i. What do you think the Full form of CGI is?
   A. Common gateway interface
   B. Client gateway interface
   C. Client gap interface
   D. Common gap interface

j. Can you clarify, Server Response with value HTTP/1.0 200 means what
   A. OK
   B. Not Found
   C. Unauthorized
   D. Forbidden

k. Can you clarify, Server Response with value HTTP/1.0 401 means what
   A. OK
   B. Not Found
   C. Unauthorized
   D. Forbidden

l. What do you think the Full Form of DNS is?
   A. Domain Name Server
   B. Data New Server
   C. Domain New Server
   D. Data Name Sever

m. Can you clarify, Which field of Email has Short Title of the message
   A. From
   B. Subject
   C. CC
   D. BCC

Skill

n. Do you know _____ describes the sources of revenue and potential benefits accruing to the involved business participants.

   A. Business Model

   B. Account Model

   C. Transaction Model

D. Inventory Model

o. Do you know _____ is the oldest catalogue of the web which is run by a loose confederation of volunteers.

A. Traditional Library

B. Virtual Library

C. Physical Library

D. Book

p. Do you know, _____ is based upon the exchange of information between individuals and organizations, over the internet.

A. Business Exchange Model

B. Traditional Exchange Model

C. Information Exchange Model

D. Discounted Exchange Model

q. Do you know, _____where companies and other organizations publish the details of their company and related information on their website.

A. Native Content Model

B. Native Transaction Model

C. Transplanted Content Model

D. Transplanted Transaction Model

r. Do you know, _____ is the one that collects a personal profile from its users and subsequently markets that data to interested set of users, while maintaining the data privacy.

A. Infomediary Model

B. Metamediaries Model

C. Data Model

D. Business Model

s. Which of the following achieves traffic aggregation for the e-retailer at almost no risk

A. Infomediary Model

B. Metamediaries Model

C. Affiliate Model

D. Business Model

t. Do you know, A new breed of internet intermediaries who provide information mediation as well as transaction support are called _____.

A. Infomediary

B. Metamediaries

C. Data

D. Business

u. How many categories are present in Transplanted Transaction Models

A. 2

B. 3

C. 4

D. 5

v. How many categories of Business models exist.

A. 2

B. 3

C. 4

D. 5

w. Do you know, Sending the same message to several users at once is called as

A. Serial Transmission

B. Broadcasting

C. Parallel Transmission

D. Unicasting

x. Do you know, A format of information which allows, in a computer environment, one to move from one part of a document to another or from one document to another through internal connections among these documents is called as

A. Hyperlink

B. Linker

C. Loader

D. Connector

y. Do you know, The header information follows a standard format of header name and the value pair, separated by which sign

A. :

B. ;

C. .

D. ,

Long Answers

Understanding

1. Explain native content based model.
2. Explain a transplanted content model.
3. Explain Digital Products Merchant Model
4. Illustrate Metamediaries model
5. Explain transplanted transaction model.
6. Illustrate e-mail concept
7. Can you explain the combination of four basic ideas in World Wide Web?
8. Illustrate the fields used in RFC 822 message format
9. Write in your own words about FTP
10. Write in you own words about different web server implementations.
11. Illustrate the steps in a typical interaction of an HTTP session with a neat diagram
12. What is a business model? Mention different categories of e-commerce business models with taxonomy diagram.

UNIT III

Multiple Choice Questions

Understanding

a. What do you think PR stands for
   A. Purchase request
   B. Purchase requisitions
   C. Purchase receipt
   D. Purchase report

b. What do you think EDI stands for
   A. Electronic Data Information
   B. Electronic Data Insurance
   C. Electronic Data Interchange
   D. Electronic Data Independent

c. What do you think EFT stands for?
   A. Electronic Fund Transport
   B. Electronic Fund Texting
   C. Electronic Fund Technology
   D. Electronic Fund Transfer

d. Can you clarify full form of DISH
   A. Data Interchange for Shopping
   B. Data Interchange for Selling
   C. Data Interchange for Shipping
   D. Data Interchange for Securing

e. Can you clarify full form of ANSI
   A. American National Standards Interchange
   B. American National Standards Information
   C. American National Standards Infrastructure
   D. American National Standards Institute

f. Can you clarify full form of Expand ISO
   A. International Standards Organization

B. Internal Standards Organization
C. Information Standards Organization
D. Institutional Standards Organization

g. Can you clarify full form of TDI
A. Traditional Data Interchange
B. Trade Data Interchange
C. Temporal Data Interchange
D. Transport Data Interchange

h. Can you clarify full form of FTP
A. File Text Protocol
B. File Transport Protocol
C. File Transfer Protocol
D. File Trait Protocol

i. Can you clarify full form of HTTP
A. Hyper Transaction Transfer Protocol
B. Hyper Trait Transfer Protocol
C. Hyper Time Transfer Protocol
D. Hyper Text Transfer Protocol

j. Can you clarify full form of VAN
A. Value-artificial network
B. Value-action network
C. Value-added network
D. Value-access network

k. What do you think DISA stands for
A. Data Interchange Standards Association
B. Data Interchange Standards Application
C. Data Interchange Standards Accessories
D. Data Interchange Standards Arrangement

l. What do you think, _____ refers to the network infrastructure that is used for the exchange of information between trading partners.

A. Interconnection layer

B. Internal layer

C. International layer

D. Information layer

m. What do you think, systems used by financial institutions are a prime example of the application of EDI in the banking and financial sector.

A. EDI

B. EFT

C. ECG

D. EGG

Application

n. Do you know, which process defines the relationship between a manufacturing organization and a consumer organization.

A. Typical trading

B. Conditional trading

C. Computer trading

D. Illegal trading

o. Do you know, _____ is the exchange of business documents between any two trading partners in a structured, machine-readable form.

A. EDI

B. EFT

C. ECG

D. EGG

p. Can you tell what is defined as any transfer of funds initiated through an electronic terminal, telephonic instrument, or computer to order, instruct or authorize a financial institution to debit or credit an account.

A. EDI

B. EFT

C. ECG

D. EGG

q. Do you know, The general architecture of the EDI system consists of how many layers.

A. Two

B. Four

C. Six

D. Eight

r. The shipping industry devised a set of standards called _____.

A. Data Interchange for Shopping

B. Data Interchange for Selling

C. Data Interchange for Shipping

D. Data Interchange for Securing

s. Do you know, which standard is promoted by the United Nations Economic Commission, which is responsible for the adoption and standardization of messages.

A. EFTFACT

B. EDIFACT

C. ECGFACT

D. EDDFACT

t. Do you know, what is a convenient method for conducting EDI which provides functionalities related to connectivity and common services

A. Value-artificial network

B. Value-action network

C. Value-added network

D. Value-access network

u. Do you know, The different transport networks interconnect using common network protocol standards is called as _____.

A. TCP/UP

B. TCP/UDP

C. TCP/DNS

D. TCP/IP

v. Can you tell, The common name space is implemented using the _____ and ensures that each machine on the internet has a unique name.

A. Domain Name System (DNS)

B. Digital Name System (DNS)

C. Demand Name System (DNS)

D. Data Name System (DNS)

w. What do you think, All published documents on the internet can be uniquely identified and located by a _____ address.

A. United Resource Locator (URL)

B. Uniform Resource Locator (URL)

C. Union Resource Locator (URL)

D. Ultra Resource Locator (URL)

x. Can you tell, Business service infrastructure includes _____.

A. Dictionaries and categories

B. Direction and categories

C. Directories and catalogues

D. Dictionaries and catalogues

y. Do you know which of the following is responsible for issuing licenses to and for regulating the certification authorities in India and maintains a directory of all the certificates as well.

A. Control of Certification Authorities (CCA)

B. Connection of Certification Authorities (CCA)

C. Categories of Certification Authorities (CCA)

D. Controller of Certification Authorities (CCA)

Long Answers

Understanding

1. Write in your own words about Electronic Data Interchange and Electronic Fund Transfer
2. Illustrate various services provided by VAN.
3. Explain the role of online payment system in E-commerce
4. Can you explain the services provided by networked multimedia content publishing in e-commerce.
5. Illustrate different protocols and their services in the network service infrastructure
6. Illustrate the essential technologies for ensuring security in an e-commerce environment?

Application

1. Analyse the building blocks of EDI system with a diagram.
2. Analyse the framework of e-commerce with a neat diagram.
3. List and analyse benefits of EDI system.
4. What are some of the direct benefits and strategic benefits of EDI.
5. What are the different application of EDI
6. Analyse the role of business service infrastructure in E-Commerce

UNIT IV

Multiple Choice Queations

Application

a. Ca you tell, Unusual attempt to gain access to a system, or to discover information about the system is called as
   - **A. Probe**
   - B. Scan
   - C. Account compromise
   - D. Packet sniffer

b. Can you tell, Large number of probes are called as
   - A. Probe
   - **B. Scan**
   - C. Account compromise
   - D. Packet sniffer

c. Can you tell, Unauthorized use of a computer account by someone other than the account owner is defined to be_____
   - **A. Account compromise**
   - B. Packet sniffer
   - C. Root compromise
   - D. Exploitation of trust

d. Which of the following Program captures data from packets as they travel over the network
   - **A. Packet sniffer**
   - B. Exploitation of Trust
   - C. Denial of services
   - D. Malicious code

e. Which among the following is Generic term for programs that cause undesired results on a system when executed
   - A. Packet sniffer
   - B. Exploitation of Trust
   - C. Denial of services
   - **D. Malicious code**

f. Can you tell, Preventing legitimate users from using a service is called as
   - **A. Denial of services**
   - B. Root compromise
   - C. Account compromise
   - D. Exploitation of trust

g. Which among the following is Self-replicating programs that spread without any human intervention, after they are started
   - A. Trojan
   - **B. Worms**
   - C. Virus
   - D. Malware

h. What is the Full form of VPN
   - **A. Virtual Private Network**
   - B. Viral Private Network
   - C. Virtual Public Network
   - D. Viral Public Network

i. Do you know which is avoidance of the unauthorized disclosure of information
   - A. Integrity
   - **B. Confidentiality**
   - C. Availability
   - D. Reliability

j. Do you know which is the computation of a function that maps the contents of a file to a numerical value.
   - **A. Checksums**
   - B. Cryptography
   - C. Confidentiality
   - D. Integrity

k. Can you tell how is the denial of a commitment or data receipt is defined as_____.
   - A. **Repudiation**
   - B. Denial of service
   - C. Probe
   - D. Disclosure

l. What is the discovery of the pattern of traffic between parties called as
   - A. Disclosure
   - **B. Traffic analysis**
   - C. Masquerade
   - D. Repudiation

m. Which of the following checks for Information alteration during its transmission over the network?
   - A. Authentication
   - **B. Integrity**
   - C. Confidentiality
   - D. Authorization

n. Do you know which among the following is the conversion of electronic data into another form, which cannot be understood by anyone except authorized parties.
   - **A. Cipher text**
   - B. Simple text
   - C. Password text
   - D. Encrypted text

o. Can you tell the Full form of PEM
   - **A. Privacy Enhanced Mail**
   - B. Privacy Enhanced Message
   - C. Public Enhanced Mail
   - D. Public Enhanced Message

p. Which among the following represents Fixed length groups of bits
   A. Blocks
   B. Group
   C. Clusters
   D. Set

q. Can you tell, the interception of information intended for someone else during its transmission over a communication channel is called as what?
   A. Eavesdropping
   B. Alteration
   C. Masquerading
   D. Repudiation

r. Can you tell Unauthorized modification of information can be called as which among the following
   A. Eavesdropping
   B. Alteration
   C. Masquerading
   D. Repudiation

s. The fabrication of information that is purported to be from someone who is not actually the author is termed as_____
   A. Eavesdropping
   B. Alteration
   C. Masquerading
   D. Repudiation

t. Do you know Conventional encryption is also called as _____
   A. **Symmetric**
   B. Asymmetric
   C. Two-way encryption
   D. Public key encryption

u. Can you tell Synonym of Asymmetric Encryption is _____
   A. Shared key
   B. Conventional encryption
   C. Public key encryption
   D. Complex key encryption

v. Which of the following RFC is used for message encryption and authentication procedures?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

w. Which of the following RFC is used for certificate based key management?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423

D. RFC 1424

x. Which of the following RFC is used for Algorithms, modes, identifiers?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

y. Which of the following RFC is used for Key certification and related services?
   A. RFC 1421
   B. RFC 1422
   C. RFC 1423
   D. RFC 1424

Long Answers

Skill

1. Find the different types of Security breaches
2. What is DOS? Can you see the possible solution where denial of service can be prevented
3. Find the different goals of Security
4. Find the different threats and attacks possible
5. What is Sniffing? Can you see the possible solution on how Sniffing can be prevented?
6. Find the different types of network transaction security issues?
7. Find what is Cyber security, and what are its type?
8. Explain the symmetric key cryptosystem with a neat diagram.
9. Explain the public key cryptosystem with a neat diagram.
10. Determine the principle of cryptography and define cipher-text
11. Find how the secret key signature key works and define digital signature
12. Find the mechanism of PGP working

UNIT V

Multiple Choice Questions

Understanding

a. What do you think, Poor e-banking planning is connected with _____

A. Strategic Risk

B. Legal Risk

C. Market Risk

D. Customer Risk

b. Can you clarify, the License to issue digital signature certificates are issued by _____

A. Finance Minister

B. Banks

C. Controller

D. User

c. Can you clarify, Key used to create digital signature is _____

A. Public key

B. Private key

C. Linear key

D. Normal key

d. What do you think, For which card one has to make advance payment?

A. Smart card

B. Gold card

C. Debit card

D. Credit card

e. What do you think, Smart cards are based in _____ standards.

A. SET

B. MIME

C. HTTP

D. TULIP

f. What do you think, Digital signature certificated are issued by _____

A. Central government

B. State government

C. Certifying authority

D. User

g. What do you think, The primary type of website used for e-banking is _____

A. Information

B. Transaction

C. Both A and B

D. Normal website

h. Can you tell, PIN in ATM card id of _____

A. 4 alphabets

B. 2 alphabets and 2 digits

C. 4 digits

D. 1 digit

i. Can you tell which one of the following is a safety measures in banking network

A. Router

B. Firewall

C. Modem

D. Switch

j. What is e-sign act?

A. Electronic sign act

B. Electronic signatures in global and national commerce act

C. Electronic signatures in national and global act

D. Electronic act

k. Who can pass the law for e-banking?

A. RBI

B. Merchant association

C. Parliament

D. State government

l. What is the full form of ATM?

A. Automatic Transaction Machine

B. Advanced Teller Machine

C. Automated Teller Machine

D. Accurate Teller Machine

m. Can you tell, Intrusion detection system helps in what?

A. User enrolment

B. Rapid intrusion detection and reaction

C. Training

D. Independent testing

Skill

n. Do you know, Payment gateways are used for what?

A. Interbank

B. Delivery process

C. Purchase

D. Client

o. Do you know, which is used to converts data transmission protocol between network

A. Gateway

B. Switch

C. Hub

D. Router

p. The customer access e-banking services using _____

A. PC

B. PDA

C. ATM

D. All of the above

q. In credit card what is the grace period of payment?

A. 10 - 15 days

B. 5 - 20 days

C. 15 - 45 days

D. 1 - 2 days

r. The most common payment especially for low value purchase, is made by _____

A. Debit card

B. Credit card

C. Cash

D. ATM

s. Transactional e-banking is typically a front end system. That realises on a programming like _____

A. Inter phase

B. Interlink

C. Inter join

D. Internal

t. Do you know, For which card one has to made advanced payments?

A. Credit card

B. Debit card

C. Smart card

D. Gold card

u. Knowing someone else password by certain illegal means is _____

A. Hacking

B. Plagiarism

C. Log on script

D. Password policy

v. Do you know, Loss of trust due to authorized activity on customer account is concerned with _____

A. Reputational risk

B. Liquidity risk

C. Market risk

D. Identity risk

w. The potential hard for informational website e-banking is _____

A. Viewing account

B. Spreading virus

C. Checking balance

D. Making online payment

x. Can you tell, A debit card/ ATM card is a _____ digit numbers.

A. 12

B. 13

C. 16

D. 10

y. Can you tell, Securer electronic transaction is a _____

A. Protocol

B. Transaction type

C. Security agency

D. JSP

Long Answers

Understand

1. Illustrate the different categories of payment systems.
2. Illustrate the different types of prepaid electronic payment systems
3. Write in your own words the major impediments faced by the mobile commerce environment.
4. Can you write a brief outline about requirement metrics of a payment system
5. Write in your own words the different activities that can be performed using M-Commerce
6. Illustrate the factors that are essential for Mobile Commerce payment

Application

7. Analyse the working of Mondex electronic payment system.
8. Analyse the working of NetBill electronic payment system.
9. What are the important revenue streams in developing business in m-commerce?
10. Analyze the architectural framework of m-commerce with a neat diagram.
11. What are the different application of M-Commerce
12. Analyze the online payment system concept