MCA(S6)22

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Housefed Complex, Dispur, Guwahati - 781 006

Master of Computer Applications

ELECTRONIC COMMERCE

CONTENTS

Subject Expert

Prof. Anjana Kakati Mahanta, Deptt. of Computer Science, Gauhati University
Prof. Jatindra Kr. Deka, Deptt. of Computer Science and Engineering,
Indian Institute of Technology Guwahati
Prof. Diganta Goswami, Deptt. of Computer Science and Engineering,
Indian Institute of Technology Guwahati

Course Coordinator

Tapashi Kashyap Das, Assistant Professor, Computer Science, KKHSOU

SLM Preparation Team

Units	Contributors
Unit 1	**Dr. Arup Goswami**, Asst. Professor, Centre for Management Studies, Dibrugarh University, Dibrugarh, Assam
Unit 2	**Pritam Medhi**, Instructor, ICT Centre, Deptt. of Disabilities Studies, Gauhati University, Assam
Unit 3 & 6	**Sangeeta Kakoty**, Asst.Professor, Deptt.of Computer Science, Jagiroad College, Morigaon, Assam
Unit 4 & 5	**Pranab Das**, Asst.Professor, Deptt. C.Sc. & E and IT, Assma Don Bosco University, Azara, Guwahati, Assam
Unit 7 & 8	**Jonalee Barman Kakati**, Asst.Professor, Deptt.of Business Administration, NERIM, Guwahati, Assam
Content Editor	**Dr. Pranjal Sarma**, Asst. Professor, Deptt.of Statistics, L.C.B.College, Guwahati

Dec 2013

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

The university acknowledges with thanks the financial support provided by the **Distance Education Council, New Delhi**, for the preparation of this study material.

Housefed Complex, Dispur, Guwahati- 781006; Web: www.kkhsou.net

COURSE INTRODUCTION

This is a course on ***Electronic Commerce***. This course is designed to provide the learners to develop skills in the electronic commerce environment.The advanced business and technological skills are valued highly in various sectors like banking, finance, accounting, auditing, information systems design, e-risk and e-assurance divisions of financial and management consulting firms etc. With this course the learners will be familier with online commerce, the Internet, and some new technologies associated with electronic commerce.

The course comprises of eight essential units. *Unit 1* is an introductory unit on electronic commerce. *Unit 2* describes how internet and web is associated with electronic commerce. *Unit 3* focuses on mobile commerce. *Unit 4* describes security issues on web. *Unit 5* provides a brief introduction to encryption and decryption techniques which are essential for security. *Unit 6* describes how intranert and extranet is related with electronic commerce. *Unit 7* explains various electronic payment systems. *Finally, Unit 8* focuses on E-Governance and law.

Each unit of this course includes some along-side boxes to help you know some of the difficult, unseen terms. Some “EXERCISES” have been included to help you apply your own thoughts. You may find some boxes marked with: “LET US KNOW”. These boxes will provide you with some additional interesting and relevant information. Again, you will get “CHECK YOUR PROGRESS” questions. These have been designed to make you self-check your progress of study. It will be helpful for you if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with “ ANSWERS TO CHECK YOUR PROGRESS” given at the end of each unit.

MASTER OF COMPUTER APPLICATIONS

Electronic Commerce

DETAILED SYLLABUS

Unit 1: Introduction to Electronic Commerce (Marks: 12)

Definition of Electronic Commerce(E-Commerce) , Scope of E-Commerce, Types of E-Commerce, Advantages of E- Commerce, Disadvantages of E-Commerce, Electronic Commerce Applications.

Unit 2: The Internet and WWW (Marks: 14)

Evolution of the Internet, The WWW and Domain Names, Registering a Domain Name, Internet Service Provider (ISP), Building a Website – Reasons and Benefits, Web Promotion, Internet Marketing and its E-cycle, Pros and Cons of online shopping.

Unit 3: Mobile Commerce (Marks: 12)

Definition of Mobile Commerce, Wireless Application Protocol(WAP), WAP technology, Mobile Information Device, Mobile Computing Applications.

Unit 4: Web Security (Marks: 14)

Security Issues on Web, Secure Transaction, Computer Monitoring, Privacy on Internet, Corporate Email Privacy, Security threats and attack on Computer System, Software Packages for Privacy, Hacking, Computer Virus, Importance of Firewall, Components of Firewall , Factors to consider Firewall design, Limitation of Firewalls.

Unit 5: Encryption and Decryption (Marks: 12)

Encryption and Decryption Techniques, Symmetric Encryption- Keys and Data Encryption Standard (DES), Triple Encryption, Asymmetric Encryption- Secret Key Encryption, Public and Private pair key encryption, Authorization and Authentication, Digital Signatures, Virtual Private Network.

Unit 6: Intranet and Extranet (Marks: 12)

Definition of Intranet, Advantages and Disadvantages of the Intranet, Component of a Intranet, Development of Intranet, Extranet and Intranet Difference, Role of Intranet in B2B Application.

Unit 7: Electronic Payment System (Marks: 12)

Overview of Electronic Payment, The SET Protocol, Payment Gateway, Payment Types, Traditional Payment, Electronic Funds Transfer, Paperless Bill, Electronic Cash, Online Banking, Concepts of EDI, EDI Application in Business, Limitations of EDI.

Unit 8: E-Governance for India and Law (Marks: 12)

E- Governance of India, Cyber Law in India, Computer Crime, Types of Crimes, Indian Custom EDI system, Service Centre, Imports, Exports, Limitations of EDI.

UNIT 1: INTRODUCTION TO ELECTRONIC COMMERCE

UNIT STRUCTURE

LEARNING OBJECTIVES

After going through this unit, you will be able to:

- learn what e-commerce is and its definition
- learn about its scope
- describe the types of e-commerce
- learn advantages and disadvantages of e-commerce
- learn various applications of e-commerce

1.2 INTRODUCTION

Electronic commerce or e-commerce has become the new mantra of modern day business world. It has emerged as the major technological development in the corporate world and has completely changed the way people do business today. The advent of internet in mid nineties has dramatically changed the socio-economic lifestyle of the entire world. The

telecommunication revolution and globalization also added to the changed perspective of human behaviour. With the rapid growth in internet applications and recent advancement in wireless and communication technology, more and more people are indulging in electronic form of business transactions. In order to cope with this modern trend of online business, the business organizations worldwide are forced to start e-commerce operations and thus increasing the scope and demand of e-commerce to a great extent.
With this unit learners will be acquainted with the concept of electronic commerce, its scope, applications as well as advantages and disadvantages.

1.3 DEFINITION OF E- COMMERCE

Electronic Commerce, or e-commerce, is the umbrella term for the entire spectrum of activities such as electronic data interchange (EDI), electronic payment system, order management, information exchange, buying and selling of products/services, and other business applications, through the electronic medium of computers/networks with electronic documentation. It is business done online. Electronic Commerce is a special technique of performing business transactions through internet using Information and Communication Technology (ICT). The business transactions involve information exchange between companies and their customers and suppliers and electronic trading of goods and services.

The e-Commerce originated in early sixties when the Electronic Data Processing (EDP) was widely used for doing business transactions. EDP provided a means for doing business operations such as order processing, payments, delivery, customer service etc. Gradually, all big corporations such as Chrysler, Ford and General Motors started to put up their own electronic network so that all their suppliers can participate in Electronic Data Interchange (EDI) over the network. EDI provided a standardized system for coding trade transactions so that they can be communicated directly from one computer system to another over the network without the need for printed orders and invoices. EDI provided a means to streamline the business procedures and improve efficiency and productivity. After the mid nineties, the private networks were gradually replaced by internet and EDI was merged to

give rise present day Electronic Commerce. Here, internet is used for commercial use like general business transactions and marketing of a wide range of goods and services.

The basic purpose of doing business through internet is to transfer business information electronically from one computer to another in an automated manner. The manual processes and paper transactions are gradually transformed to online versions to help people operate in a fully electronic environment. This in turn gives rise to a new concept called Electronic Market. An Electronic Market is an inter-organizational information system that provides facilities for buyers and sellers to exchange information about price and products. The information sharing could be done effectively through the internet. The purpose of the electronic market is to make people across the world familiar with the range of products of their interest. An effective electronic market increases the efficiency of the market as it reduces the search cost for the buyer.

The direct interaction between consumers and manufacturers through a common platform called electronic market reduces the role of intermediaries or middlemen and ultimately reduces the cost of distribution. Thus, the electronic commerce has an important impact on our economy.

1.4 SCOPE OF E- COMMERCE

The scope of e-commerce includes the following elements of a business process:

- Information Exchange
- Order Placement
- Payment and Delivery
- Customer Service
- Marketing

The Information Exchange part includes development of Web Site containing details of products/services and electronic catalogues providing detailed information on pricing, quality and delivery and payment terms. In some cases it may include banner advertisement and customized offering through interaction via electronic mail.

After deciding to buy a particular product/service the customer enters the second phase, namely the Order Placement phase. Here the customer negotiates the final payment, delivery and service options and formalizes the contract.

The Order Placement phase is followed by Payment and Delivery which involves shipment of goods and subsequent payment. The payment in electric commerce can be done through traditional means such as using credit cards over the networks or utilizing electronic fund transfer involving digital cash. In the case of electronic goods such as software packages, digitized music clips or video clips and other multimedia information in digital format, the shipment or delivery is done instantaneously over the network. In the case of physical goods, once the payment is validated online, the physical shipment is done in consultation with the buyer.

The Customer Service phase in electronic commerce involves direct link between customer and supplier. In electronic commerce system the customer and product/service providers are directly connected through the internet. Thus the customers remain automatically updated regarding the latest product/service information as well as they get instantaneous access to any service required for any kind of problems. This direct reach to the service provider leads to a major source of efficiency in electronic commerce.

The Marketing part utilizes the data generated by customer support along with any other feedback or preferences. This in turn will lead to strategic planning for improved product/service or new product offering.

The scope of electronic commerce is thus to encompass all the above business activities in a broader perspective than just buying and selling through internet. The direct connectivity between suppliers and customers lead to improved service and reduction of time and cost. All the above

activities when integrated to the information system infrastructure of the organization results to much improved performance and higher profit and productivity.

CHECK YOUR PROGRESS - 1

Q.1. State true or false for the following statement:

i. Electronic commerce is a special technique of performing business transactions through internet.

ii. The e-commerce originated in early seventies.

iii. Electronic Market is an Inter-organisational information system that provides facilities for buyers and sellers to exchange information about price and product through internet.

iv. E-commerce increases the cost of distribution.

v. EDP means Electronic Data Processing.

1.5 TYPES OF E-COMMERCE

There are variety of different types of e-commerce and many different ways to characterize these types. Different types of e-commerce may be distinguished by the nature of the market relationship—who is selling to whom. The exceptions are P2P and m-commerce, which are technology-based distinctions.

B2C: The most commonly discussed type of e-commerce is Business-to-Consumer (B2C) e-commerce, in which online businesses attempt to reach

individual consumers. Even though B2C is comparatively small, it has grown exponentially since 1995, and is the type of e-commerce that most consumers are likely to encounter. Within the B2C category there are many different types of business models. There are seven different B2C business models: portals, online retailers, concept providers, transaction brokers, market creators, service providers and community providers.

B2B: Business-to-business (B2B) e-commerce is the largest form of e-commerce, in which businesses focus on selling to other businesses. B2B e-commerce has significant growth potential. The size of B2B e-commerce could be huge. Initially, B2B e-commerce primarily involved inter-business exchanges, but a number of other B2B business models have developed, including e-distributors, B2B service providers, matchmakers, and infomediaries that are widening the use of B2b e-commerce.

C2C: Consumer-to-Consumer (C2C) e-commerce provides a way for consumers to sell to each other, with the help of an online market maker such as the auction site e-Bay. In C2C e-commerce, the consumer prepares the product for market, places the product for auction or sale, and relies on the market maker to provide catalog, search engine, and transaction-clearing capabilities so that products can be easily displayed, discovered, and paid for.

P2P: Peer-to-peer technology enables Internet users to share files and computer resources directly without having to go through a central Web server. In peer-to-peer's purest form, no intermediary is required. For instance, Gnutella is a peer-to-peer freeware software application that permits users to directly exchange musical tracks, typically without any charge. Since 1999, entrepreneurs and venture capitalist have attempted to adapt various aspects of peer-to-peer technology into peer-to-peer (P2P) e-commerce. Napster.com, which was established to aid Internet users in finding and sharing online music files known as MP3 files, is most well known example of peer-to-peer e-commerce. Later in 2000, the Recording Industry of America, a trade organization of the recording companies, successfully sued Napster for violating copyright law by allowing Napster members to exchange copyrighted music tracks without compensation to the copyright holders.

M-commerce: Mobile commerce or m-commerce refers to the use of wireless digital devices to enable transactions on the Web. These devices utilize wireless networks to connect cell phones and handheld devices to the Web. Once connected, mobile consumers can conduct many types of transactions including banking, travel reservations etc.

G2G/G2B/G2C:(E-governance)Government-to-Government/Government-to-Business/
Government-to-Consumer: E-Governance refers to the application of Information and Communication Technology (ICT) in governance processes and functions. The purpose of e-governance is to improve the quality and accessibility of existing government products and services to the common people and also to generate new products and services. Application of Information Technology enhances the participation of common people in the governance procedures and also improves the scope and choices of government services. Another important aspect of e-governance is that it makes it possible to include some special sections of society, such as poor, illiterate, migrants and disabled, who are most likely to be excluded from various government procedures in various developmental programs. Application of ICT in performing administrative functions of various government departments cater to larger number of people across different geographical locations. Effective use of ICT can greatly improve the efficiency of services, reduce the communication cost and improve the transparencies in functioning of various departments.
Government of India has started various e-governance projects in both central and state level to facilitate e-governance. These include G2G, G2B and G2C services in various departments and industry sectors. E-governance in India includes online application filing, bill payment, tax collection, distance education, tele-medicine etc.

B2G: In Business-to-Government e-commerce government organizations are involved in online purchase of various materials from business organizations. The online procurement results in substantial cost cutting of the government establishments which is reflected in rapid growth of online government procurement in recent years. E-procurement is a special component of B2G where government agencies announce request for proposal on their own

website for suppliers to bid on each proposal by e-mail or through the website. The potential savings in time and cost could be quite impressive.

B2A: Business-to- Administrator/ Business-to-Anyone

C2B: Consumer-to-Business e-commerce deals with the transaction between individual consumers and business organizations where the consumer originates the transaction by specifying the price of a particular commodity. C2B enables buyers to quote their own price for a product or service and thus generating demand. The website collects the demand bids and then offers the bids to the particular sellers. Here the consumers get a choice of a wide variety of commodities and services along with the opportunity to specify the range of prices they can afford or are willing to pay. It reduces the bargaining time, increases the flexibility for both the consumer and the merchant. Examples of C2B are RevenueAuction.com, priceline.com etc.

1.6 ADVANTAGES OF E-COMMERCE

The internet has made many things easier such as communicating with friends and family and banking. It saves time which in this day and time is a big convenience. The internet has allowed the development of online business which sells their product to a worldwide audience. The spread of e-commerce will depend on the perception of the consumer of its advantages and disadvantages. The perception depends, in part at least, on the individual, their circumstances and the goods or services that are to be traded.

Among the advantages of e-commerce for both the consumer and the traders are:

- **Low cost:** Online business does not have overheads associated with a shop. Therefore they often have lower prices than a traditional shop.
- **Home Shopping:** Shopping can be done from the comfort of home, hopefully quickly and conveniently. E-commerce allows the consumers to avoid the hassles of travelling, parking, and queuing.

- **World-wide, 24 Hours a Day Trading**: The shopper can access an e-shop anywhere in the world at any time day or night rather than having to visit during business hours. This is particularly handy for shift workers, people in remote areas or people with limited ability to leave the house including those with young children. Internet can be used to research the product and compare prices more easily than visiting several different stores before actual purchase. In online dealings there are no chances of dealing a sales person who talk to trying additional sales.
- **The Latest Thing at Bargain Prices**: Goods bought online may be competitively priced and more up-to-date than goods available in a conventional retail shop.
- **Home Delivery**: The goods are delivered at the door step of the buyer.
- **Online Sales Support**: For some goods there can be information online on how to use them and how to fix them. E-mail can also be an appropriate facility for after-sales services.

1.7 DISADVANTAGES OF E- COMMERCE

Disadvantages of e-commerce include the following:

- **Privacy and Security**: The privacy of personal details and security of financial transactions are a concern to many users and potential users of e-commerce.
- **Delivery**: Where tangible goods are bought online they have to be delivered. Delivery may be at extra cost. In case of overseas delivery the cost may be further higher due to difference of conversion rate and international transaction fee charges.
- **Inspecting Goods**: The web can provide a good picture, description and even customer reviews but cannot be actually seen, feel or try on the goods purchased. Therefore, ascertaining quality, make, size etc. are difficult in online shopping.

- **Social Interaction**: Shopping for some is a chore and for others is an outing. A shopping trip on the internet will not be the same experience as a shopping expedition with family members or friends for those who likes to go out.
- **Return of Goods**: Returning faulty goods to an online vendor is time consuming and is an problematic affair.

1.8 ELECTRONIC COMMERCE APPLICATIONS

Electronic commerce can be applied in the following fields:

- **Online Publishing:** Online publishing facilitates production, processing, storage and distribution of books and magazines in digitalized format over the internet. The online news papers and magazines are becoming popular in households across the globe and are gradually replacing offline newspapers. Another important application of online publishing is in the area of education and training. Computer based education has become very common in developing countries where people in remote places get the advantage of accessing quality education with the help of internet. The digitized course materials are distributed and live video conferencing through internet makes it possible to conduct classes by highly skilled professionals at a relatively low cost.

- **Internet Bookshops**: Internet bookshops are online publishing or distribution houses that publish, sell and distribute book as well as digitized versions of books over the internet. The websites of these bookstores display the catalogs of books along with the pricing information for customer reference. The online order form is available and online payment is accepted. The books in digitized form can be downloaded directly from the internet while book are physically delivered to the customers once the payment is accepted.

- **Electronic Newspaper**: Electronic Newspapers publish newspaper contents in their websites along with the pictures and classified ads. The browser displays the headlines 24X7 and on a timely manner. The online newspapers do not have to wait for the offline newspaper to be printed and delivered at their home till the morning comes. Instead, the online newspaper shows the news instantly in the computer screen. Whenever there is breaking news, the online newspapers update and upload in their websites, eliminating the time bound printing and delivery process. In this respect the online newspapers compete directly with television and radio for reporting breaking news. Another advantage of online newspaper is that they offer access to their news archives by extensive search facilities for searching back issues. The major revenue for online newspapers comes from classified Ads appearing in the newspaper websites. The supply chain of online newspapers is relatively simpler than conventional newspapers as the time consuming printing and delivery is absent. The content is developed and uploaded directly in the web eliminating the cumbersome packaging and delivery process.

- **Online Education**: Online Education is the form of distance education which is facilitated by computer programmes, video instructions, educational television programmes or satellite courses to provide educational opportunities to students who are unable to attend university courses due to remote locations, physical disability or timing conflicts. The online courses are broadcast either by internet or satellite TV channels at student convenience. The electronic versions of course materials are available online and courses are delivered in audio-visual mode to stimulate a virtual classroom. The electronic access to online databases as well as library catalogs eliminates the use of books or reference materials but requires substantial computer disk space. The use of educational CD ROMS has an impact on the learning process and the successful implementation of electronic commerce technology is required to support the online education system. The advantages of online education includes:

  Place independence: One of the advantages of online education is that it is place independent. Students can attend

online courses while travelling through their laptop computers, complete assignments at their home and submit by uploading through the internet from any distant location.

Time independence: Online education is also time independent. To and fro communication can be maintained with the help of e-mail without both the parties available in real time. It is helpful to the busy working adults.

The main disadvantage of online education is the lack of direct contract with the faculties may not provide the required quality of teaching to certain students which may be possible in class room teaching.

- **Internet Banking:** Internet banking, also known as Online Banking allows customers to conduct financial transactions, check their account balance or pay a bill through the bank website in a secured manner at anytime of the day and from anywhere on the globe. Online banking works in the same manner as traditional banking. The main difference is that, instead of going down to the local bank branch office physically, the customers can perform multiple banking tasks such as accessing account information, bill payment or transfer funds from their home or office using computers and internet. However for getting cash or depositing cash to the bank one has to go to the bank branch or Automated Teller Machine (ATM). Through online banking, one can have easy and instant access of account balance, make bill payment, transfer money between accounts and download details of account transactions. Some banks offer additional online banking facilities such as phone banking, online share trading etc.

  The online banking offers many advantages—Users can conduct banking operations 24 hours a day from their home or anywhere even on holidays. It is cost effective too as thousands of customers can be served simultaneously and automatically.

E-Commerce also helps in developing rural markets. Several companies have created virtual bazaars or agri-portals akin to the

weekly mandis (weekly markets). The notable ones are e-Choupal by ITC, India Agriline by EID Parry and the dairy portal by Amul.

CHECK YOUR PROGRESS-2

2Q. Fill in the blanks with appropriate words:

i. E-Governance refers to application of Information and Communication Technology (ICT) in _____ processes and functions.
ii. P2P refers to _____ e-commerce.
iii. E-Commerce helps to _____ the hassles of travelling, parking and queuing.
iv. In E-Commerce mode it is _____ to ascertaining quality, size etc. of a commodity.

1.9 LET US SUM UP

In this unit we have discussed about the electronic commerce. Electronic Commerce, or e-commerce, is the umbrella term for the entire spectrum of activities such as electronic data interchange (EDI), electronic payment system, order management, information exchange, buying and selling of products/services, and other business applications, through the electronic medium of computers/networks with electronic documentation. There are many types of e-commerce. Some of them are C2C, G2G, B2G, B2P, P2P

etc. Electronic commerce offers many advantages like low cost, ease of shopping from home etc. but there are some disadvantages of e-commerce too like privacy problem, lack of opportunity of inspecting quality etc. Few major application of e-commerce are distance education, internet banking, internet bookshop, e-newspaper etc.

1.10 FURTHER READINGS

1. E-Commerce Past, Present and Future by Karabi Bandyopadhyay, Vrinda Publications (P) Ltd., New Delhi, 2012
2. E-Commerce—Strategy, Technologies and Applications by David Whiteley,Tata McGraw—Hill Publishing Company Limited, New Delhi, 2006
3. E-Commerce Business, Technology, Society by Kenneth C. Laudon, and Carol Guercio Traver, Pearson Education, New Delhi, 2008

1.11 ANSWERS TO CHECK YOUR PROGRESS

1. (i) True (ii) False (iii) True (iv) False (v) True
2. (i) governance (ii) peer-to-peer (iii) avoid (iv) difficult

1.12 MODEL QUESTIONS

Q1. Define e-commerce.
Q2. Discuss the scope of e-commerce.
Q3. Explain briefly the various types of e-commerce.
Q4. Writes short notes on: (a) B2C; (b) P2P; (c) C2C
Q5. Enumerate the advantages and disadvantages of e-commerce.
Q6. Discuss in brief the various applications of e-commerce.
Q7. What do you understand by internet banking?

*****

UNIT 2: THE INTERNET AND WWW

UNIT STRUCTURE

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- give a brief history of internet.
- learn about WWW, domain name and registering a domain name.
- learn the ways of promoting website
- learn the reasons for creating a website
- learn about the concept of internet marketing
- learn about online shopping and its pros and cons

2.2 INTRODUCTION

In the first unit of this paper you were introduced to the different concepts of Electronic Commerce, its functions, impact, advantages etc. The various applications and functionalities of all the components that are related to E-commerce were also discussed in detail. In this unit we will deal with one of the most important and relevant concept of modern day computing which is called the internet. Internet today holds importance in almost all walks of our lives like reading the morning newspaper, watching our favorite television programs online, viewing live cricket, E-learning, E-business etc. In this unit we will learn the various concepts that are used in the various applications of the internet.

We start this unit by discussing about the evolution of the internet, explaining all the various essential terminologies that need to be understood in order to have a firm grasp on the various applications running on the internet. Domain names which are in existence for every website present on the internet are also discussed, as to how to own and register a domain. The concept of promoting a website after it is developed has also been discussed in this unit. Promoting a website, involves creating ways by which the longevity of a website's existence can be increased, and the process of doing so involves creating and developing ways for maximizing a website's throughput. We also delve on the concepts of internet marketing and online shopping and discuss their merits and demerits.

2.3 EVOLUTION OF THE INTERNET

The Internet has revolutionized the world of computers and communications in a manner that almost every task in today's world is internet-driven. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet can be termed as a world-wide broadcasting capability, a mechanism for information propagation, and a medium for association and communication between individuals and their computers regardless of their geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure.

The history of the Internet began in the 1950s with the development of electronic computers. The first message was sent over the **ARPANet**, which evolved into the internet, from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA), after the second piece of network

equipment was installed at Stanford Research Institute (SRI). Packet switched networks such as **ARPANET, Mark I** at NPL in the UK, CYCLADES, Merit Network, Tymnet, and Telenet, were developed in the late 1960s and early 1970s using a variety of protocols. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined together into a network of networks.

In 1982, the Internet protocol suite **(TCP/IP)** was standardized, and consequently, the concept of a world-wide network of interconnected TCP/IP networks, called the Internet, was introduced. Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) developed the Computer Science Network (CSNET) and again in 1986 when NSFNET provided access to supercomputer sites in the United States from research and education organizations. Commercial Internet service providers (ISPs) began to emerge in the late 1980s and early 1990s. The ARPANET was decommissioned in 1990. The Internet was commercialized in 1995 when NSFNET was decommissioned, removing the last restrictions on the use of the Internet to carry commercial traffic.

Since the mid-1990s, the Internet has had a revolutionary impact on culture and commerce, including the rise of near-instant communication by electronic mail, instant messaging, Voice over Internet Protocol (VoIP) "phone calls", two-way interactive video calls, and the World Wide Web with its discussion forums, blogs, social networking, and online shopping sites. The research and education community continues to develop and use advanced networks such as NSF's very high speed Backbone Network Service (vBNS), Internet2, and National LambdaRail. Increasing amounts of data are transmitted at higher and higher speeds over fiber optic networks operating at 1-Gbit/s, 10-Gbit/s or more. The Internet's takeover of the global communication landscape was almost instant in historical terms: it only communicated 1% of the information flowing through two-way telecommunications networks in the year 1993, already 51% by 2000, and more than 97% of the telecommunicated information by 2007. Today the Internet continues to grow, driven by ever greater amounts of online information, commerce, entertainment and social networking.

2.4 THE WWW AND DOMAIN NAMES

WWW –

The **World Wide Web** (abbreviated as **WWW** or **W3**, commonly known as **the web**) is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks. In March 1989 Tim Berners-Lee, a British computer scientist and former CERN employee, wrote a proposal for what would eventually become the World Wide Web. The 1989 proposal was meant for a more

effective CERN communication system but Berners-Lee eventually realised the concept could be implemented throughout the world. Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "to link and access information of various kinds as a web of nodes in which the user can browse at will", and Berners-Lee finished the first website in December of that year. The terms Internet and World Wide Web are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not the same. The Internet is a global system of interconnected computer networks. In contrast, the web is one of the services that runs on the Internet. It is a collection of text documents and other resources, linked by hyperlinks and URLs, usually accessed by web browsers from web servers. In short, the web can be thought of as an application "running" on the Internet.

Viewing a web page on the World Wide Web normally begins either by typing the URL of the page into a web browser or by following a hyperlink to that page or resource. The web browser then initiates a series of communication messages in order to fetch and display it. In the 1990s, using a browser to view web pages—and to move from one web page to another through hyperlinks—came to be known as 'browsing,' 'web surfing,' or 'navigating the web'. Early studies of this new behavior investigated user patterns in using web browsers.

The following example demonstrates how a web browser works. Consider accessing a page with the URL http://example.org/home/World_Wide_Web.

First, the browser resolves the server-name portion of the URL (*example.org*) into an Internet Protocol address using the globally distributed database known as the Domain Name System (DNS); this lookup returns an IP address such as *208.80.152.2*. The browser then requests the resource by sending an HTTP request across the Internet to the computer at that particular address. It makes the request to a particular application port in the underlying Internet Protocol Suite so that the computer receiving the request can distinguish an HTTP request from other network protocols it may be servicing such as e-mail delivery; the HTTP protocol normally uses port 80. The content of the HTTP request can be as simple as the two lines of text GET */home/* World_Wide_Web HTTP/1.1 Host: *example.org*

The computer receiving the HTTP request delivers it to web server software listening for requests on port 80. If the web server can fulfill the request it sends an HTTP response back to the browser indicating success, which can be as simple as HTTP/1.0 200 OK Content-Type: text/html; charset=UTF-8 followed by the content of the requested page. The Hypertext Markup Language for a basic web page looks like `<html> <head> <title>Example.org – The World Wide Web</title> </head> <body> <p>The World Wide Web, abbreviated as WWW and commonly known ...</p> </body> </html>`. The web browser parses the HTML, interpreting the markup (<title>, <p> for paragraph, and such) that surrounds the words in order to draw the text on the screen.

Many web pages use HTML to reference the URLs of other resources such as images, other embedded media, scripts that affect page behavior, and Cascading Style Sheets that affect page layout. The browser will make additional HTTP requests to the web server for these other Internet media types. As it receives their content from the web server, the browser progressively renders the page onto the screen as specified by its HTML and these additional resources. Many host names used for the World Wide Web begin with *www* because of the long-standing practice of naming Internet hosts (servers) according to the services they provide. The host name for a web server is often *www*, in the same way that it may be *ftp* for an FTP server, and *news* or *nntp* for a USENET news server. These host names appear as Domain Name System or (DNS) subdomain names, as in www.example.com. According to Paolo Palazzi, who worked at CERN along with Tim Berners-Lee, the popular use of 'www' subdomain was accidental; the World Wide Web project page was intended to be published at www.cern.ch while info.cern.ch was intended to be the CERN home page, however the dns records were never switched, and the practice of prepending 'www' to an institution's website domain name was subsequently copied. Many established websites still use 'www', or they invent other subdomain names such as 'www2', 'secure', etc. Many such web servers are set up so that both the domain root (e.g., example.com) and the *www* subdomain (e.g., www.example.com) refer to the same site; others require one form or the other, or they may map to different web sites. The use of a subdomain name is useful for load balancing incoming web traffic by creating a CNAME record that points to a cluster of web servers. Since, currently, only a subdomain can be used in a CNAME, the same result cannot be achieved by using the bare domain root.

When a user submits an incomplete domain name to a web browser in its address bar input field, some web browsers automatically try adding the prefix "www" to the beginning of it and possibly ".com", ".org" and ".net" at the end, depending on what might be missing. For example, entering 'microsoft' may be transformed to *http://www.microsoft.com/* and 'openoffice' to *http://www.openoffice.org*.

Use of the www prefix is declining as Web 2.0 web applications seek to brand their domain names and make them easily pronounceable. As the mobile web grows in popularity, services like Gmail.com, MySpace.com, Facebook.com and Twitter.com are most often discussed without adding www to the domain (or, indeed, the .com).

Domain names –

A **domain name** is an identification string that defines a realm of administrative autonomy, authority or control on the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name. Domain names are used in various networking contexts and application-specific naming and addressing purposes. In general, a domain name represents an Internet

Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), such as the prominent domains com, info, net, edu, and org, and the country code top-level domains (ccTLDs). Below these top-level domains in the DNS hierarchy are the second-level and third-level domain names that are typically open for reservation by end-users who wish to connect local area networks to the Internet, create other publicly accessible Internet resources or run web sites. The registration of these domain names is usually administered by domain name registrars who sell their services to the public. A fully qualified domain name (FQDN) is a domain name that is completely specified in the hierarchy of the DNS, having no omitted parts. Domain names are usually written in lowercase, although labels in the Domain Name System are case-insensitive. Domain names serve as more easily memorable names for Internet resources such as computers, networks, and services. Individual Internet host computers use domain names as host identifiers, or host names. Host names are the leaf labels in the domain name system usually without further subordinate domain name space. Host names appear as a component in Uniform Resource Locators (URL's) for Internet resources such as web sites. Domain names are also used as simple identification labels to indicate ownership or control of a resource. Such examples are the realm identifiers used in the Session Initiation Protocol (SIP), the Domain Keys used to verify DNS domains in e-mail systems, and in many other Uniform Resource Identifiers (URIs).

An important function of domain names is to provide easily recognizable and memorizable names to numerically addressed Internet resources. This abstraction allows any resource to be moved to a different physical location in the address topology of the network, globally or locally in an intranet. Such a move usually requires changing the IP address of a resource and the corresponding translation of this IP address to and from its domain name. Domain names are used to establish a unique identity. Organizations can choose a domain name that corresponds to their name, helping Internet users to reach them easily. Generic domain names increase popularity. A generic domain name may sometimes define an entire category of business that a company is involved in, rather than being the name of the company. Some examples of generic names include books.com, music.com, travel.com and art.com. Companies have created successful brands based on a generic name, and such generic domain names tend to be very valuable. Domain names are often referred to simply as *domains* and domain name registrants are frequently referred to as *domain owners*, although domain name registration with a registrar does not confer any legal ownership of the domain name, only an exclusive right of use. The use of domain names in commerce may subject them to trademark law.

CHECK YOUR PROGRESS

1. Fill in the blanks

(a) The _____ can be termed as a world-wide broadcasting capability.

(b) One can view web pages with _____ and navigate between them via _____.

(c) A web page can be viewed by typing the ____ of the page or by following a _____ to that page or resource.

(d) Domain names are formed by the rules and procedures of the _____.

(e) A domain name represents an _____ resource.

2.5 REGISTERING A DOMAIN NAME

The first commercial Internet domain name, in the TLD *com*, was registered on 15 March 1985 in the name symbolics.com by Symbolics Inc., a computer systems firm in Cambridge, Massachusetts. By 1992, fewer than 15,000 *com* domains had been registered. In December 2009, 192 million domain names had been registered.

The right to use a domain name is delegated by domain name registrars, which are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN), the organization charged with overseeing the name and number systems of the Internet. In addition to ICANN, each top-level domain (TLD) is maintained and serviced technically by an administrative organization operating a

registry. A registry is responsible for maintaining the database of names registered within the TLD it administers. The registry receives registration information from each domain name registrar authorized to assign names in the corresponding TLD and publishes the information using a special service, the WHOIS protocol. Registries and registrars usually charge an annual fee for the service of delegating a domain name to a user and providing a default set of name servers. Often, this transaction is termed a sale or lease of the domain name and the registrant may sometimes be called an "owner", but no such legal relationship is actually associated with the transaction, only the exclusive right to use the domain name. More correctly, authorized users are known as "registrants" or as "domain holders". ICANN publishes the complete list of TLD registries and domain name registrars. Registrant information associated with domain names is maintained in an online database accessible with the WHOIS protocol. For most of the 250 country code top-level domains (ccTLDs), the domain registries maintain the WHOIS (Registrant, name servers, expiration dates, etc.) information. Some domain name registries, often called *network information centers* (NIC), also function as registrars to end-users. The major generic top-level domain registries, such as for the COM, NET, ORG, INFO domains and others, use a registry-registrar model consisting of hundreds of domain name registrars. In this method of management, the registry only manages the domain name database and the relationship with the registrars. The *registrants* (users of a domain name) are customers of the registrar, in some cases through additional layers of resellers.

In the process of registering a domain name and maintaining authority over the new name space created, registrars use several key pieces of information connected with a domain:

- **Administrative contact –** A registrant usually designates an administrative contact to manage the domain name. The administrative contact usually has the highest level of control over a domain. Management functions delegated to the administrative contacts may include management of all business information, such as name of record, postal address, and contact information of the official registrant of the domain and the obligation to conform to the requirements of the domain registry in order to retain the right to use a domain name. Furthermore the administrative contact installs additional contact information for technical and billing functions.
- **Technical contact –** The technical contact manages the name servers of a domain name. The functions of a technical contact include assuring conformance of the configurations of the domain name with the requirements of the domain registry, maintaining the domain zone records, and providing continuous functionality of the name servers (that leads to the accessibility of the domain name).
- **Billing contact –** The party responsible for receiving billing invoices from the domain name registrar and paying applicable fees.

- **Name servers –** Most registrars provide two or more name servers as part of the registration service. However, a registrant may specify its own authoritative name servers to host a domain's resource records. The registrar's policies govern the number of servers and the type of server information required. Some providers require a hostname and the corresponding IP address or just the hostname, which must be resolvable either in the new domain, or exist elsewhere. Based on traditional requirements (RFC 1034), typically a minimum of two servers is required.

Domain names may be formed from the set of alphanumeric ASCII characters (a-z, A-Z, 0-9), but characters are case-insensitive. In addition the hyphen is permitted if it is surrounded by characters or digits, i.e., it is not the start or end of a label. Labels are always separated by the full stop (period) character in the textual name representation.

2.6 INTERNET SERVICE PROVIDER

An **Internet service provider** (**ISP**), also called telephone companies or other telecommunication providers, provides services such as Internet access, Internet transit, domain name registration and hosting, dial-up access, leased line access and collocation. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

Classification of ISPs

1) Access providers –

- Access ISPs employ a range of technologies to enable consumers to connect to their network. Over time, available technologies have ranged from acoustic couplers to telephone lines, to cable, wi-fi, and fiber optics.
- For users and small businesses, traditional options include copper wires to provide dial-up, DSL (typically asymmetric digital subscriber line, ADSL), cable modem or Integrated Services Digital Network (ISDN) (typically basic rate interface). Using fiber-optics to end users is called Fiber To The Home or similar names.
- For customers with more demanding requirements, such as medium-to-large businesses, or other ISPs, higher-speed DSL (such as single-pair high-speed digital subscriber line), Ethernet, metropolitan Ethernet, gigabit Ethernet, Frame Relay, ISDN Primary Rate Interface, ATM (Asynchronous

Transfer Mode) and synchronous optical networking (SONET) can be used.

- Wireless access is another option, including satellite Internet access.
- Many access providers also provide hosting and email services.

2) Mailbox providers –

- A **mailbox provider** is a department or organization that provides email mailbox *hosting* services. It provides email servers to send, receive, accept and store email for other organizations and/or end users, on their behalf and upon their explicit mandate.
- Many mailbox providers are also access providers, while others are not (e.g., Yahoo! Mail, Hotmail, Gmail, AOL Mail, Pobox). The definition given in RFC 6650 covers email hosting services, as well as the relevant department of companies, universities, organizations, groups, and individuals that manage their mail servers themselves. The task is typically accomplished by implementing Simple Mail Transfer Protocol (SMTP) and possibly providing access to messages through Internet Message Access Protocol (IMAP), the Post Office Protocol, Webmail, or a proprietary protocol.

3) Hosting ISPs –

Hosting ISPs routinely provide email, FTP, and web-hosting services. Other services include virtual machines, clouds, or entire physical servers where customers can run their own custom software.

- **Transit ISPs –**

Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP and/or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to. In the simplest case, a single connection is established to an upstream ISP and is used to transmit data to or from areas of the Internet beyond the home network; this mode of interconnection is often cascaded multiple times until reaching a Tier 1 carrier. In reality, the situation is often more complex. ISPs with more than one point of presence (PoP) may have separate connections to an upstream ISP at multiple PoPs, or they may be customers of multiple upstream ISPs and may have connections to each one of them at one or more point of presence. Transit ISPs provide large amounts of bandwidth for connecting hosting ISPs and access ISPs.

- **Virtual ISPs –**

A virtual ISP (VISP) is an operation which purchases services from another ISP (sometimes called a "wholesale ISP" in this context) which allow the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP. It is akin to mobile virtual network operators and competitive local exchange carriers for voice communications.

- **Free ISPs –**

Free ISPs are Internet service providers which provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial television, in a sense they are selling the users' attention to the advertiser. Other free ISPs, often called free nets, are run on a nonprofit basis, usually with volunteer staff.

2.7 BUILDING A WEBSITE – REASONS AND BENIFITS

Building or designing your own website gives you a professional edge. By building or creating a website of your own you are at once placing yourself ahead of everybody else. The following are some of the reasons why one would like to build one's own website.

Reasons for building a website –

There are many varied reasons as to why one would like to build ones own website. Some of them are as follows.

1) Building an Internet presence through a domain name of your own choice could be one reason as to why building a website could be necessary. By having your own website with your own domain name, you can start to build your own "brand" that will eventually become recognized as uniquely yours. This will make you stand out from the crowd of people all promoting the same products through identical affiliate websites.
2) Building your own website with your own domain name looks more professional than many affiliate sites. Many affiliate websites that you can promote may not look that good. If you build your own website to promote a product or service, you can make it look just how you want, and this can include targeting it at a specific niche or customer segment.
3) Once you have your own domain name, you can then have a more professional looking email address. Most Internet users will have either an email address with their Internet Service Provider (e.g. markfarrar@aol.com) or a Hotmail or

Yahoo email address, but these do not look very professional if you are trying to run a business.

4) It is a good way of disguising affiliate links and therefore stopping people from robbing you of your commissions. Many affiliate website links look untidy or are too long, and, worst of all, they look like affiliate links. Some people have an unexplainable aversion to purchasing something through an affiliate. Worse still, people can easily alter the affiliate URL and add their own affiliate id, resulting in you losing commissions. A better approach is to build a page on your own website that redirects to the affiliate program behind the scenes, as this hides the affiliate link completely.

5) You can promote more than one product or service at the same time. Although some experts recommend that you should promote only one product per page, this is not always practical. If you have your own website, you can list related products on one page, even if they are from different companies. Again, this comes down to offering what your customers will be looking for.

6) You get to control cross-sell and up-sell opportunities. Depending on what you sell and how, you can offer an "upsell" opportunity as part of the sales process. This may be a special offer. For example, that the customer only sees once, and this creates a sense of urgency that is a proven and powerful incentive to buy.

7) You can build a mailing list of your own. If you capture people's contact details (first name and email address are the absolute minimum), you can then send other offers to your mailing list whenever you want.

8) It is really very easy to build a good-looking website, only by using specialist website-building software, but all you really need is the Notepad program that comes with Windows and a good website or book to learn from.

9) Earning revenues is the main reason for building a website, whereby revenue can be earned by sponsoring, promoting, advertising and running several affiliate programs that are meant for sponsorship purposes.

10) There is something extremely satisfying about seeing your own creation come to life and knowing that your website is available to several million potential customers the moment you publish it on the Internet.

2.8 WEB PROMOTION

Website Promotion is the continuing process used by webmasters to promote and bring more visitors to a website. Many techniques such as web content development, search engine

optimization, and search engine submission, are used to increase a site's traffic.

Web Content Development –

It is the process of researching, writing, gathering, organizing, and editing information for publication on web sites. Web site content may consist of prose, graphics, pictures, recordings, movies or other digital assets that could be distributed by a hypertext transfer protocol server, and viewed by a web browser. When the World Wide Web began, web developers either generated content themselves, or took existing documents and coded them into hypertext markup language (HTML). In time, the field of web site development came to encompass many technologies, so it became difficult for web site developers to maintain so many different skills. Content developers are specialized web site developers who have content generation skills such as graphic design, multimedia development, professional writing and documentation. They can integrate content into new or existing web sites without using information technology skills such as script language programming and database programming. Content developers may also be search engine optimization specialists, or Internet marketing professionals. High quality, unique content is what search engines are looking for and content development specialists therefore have a very important role to play in the search engine optimization process. One issue currently plaguing the world of web content development is keyword-stuffed content which are prepared solely for the purpose of manipulating a search engine. This is giving a bad name to genuine web content writing professionals. The effect is writing content designed to appeal to machines (algorithms) rather than people or community. Search engine optimization specialists commonly submit content to Article Directories to build their website's authority on any given topic. Most Article Directories allow visitors to republish submitted content with the agreement that all links are maintained. This has become a method of Search Engine Optimization for many websites today. If written according to SEO copywriting rules, the submitted content will bring benefits to the publisher (free SEO-friendly content for a webpage) as well as to the author (a hyperlink pointing to his/her website, placed on an SEO-friendly webpage).

Search Engine Optimization –

Search Engine Optimization (**SEO**) is the process of affecting the visibility of a website or a web page in a search engine's "natural" or un-paid ("organic") search results. In general, the earlier (or higher ranked on the search results page), and more frequently a site appears in the search results list, the more visitors it will receive from the search engine's users. SEO may target different kinds of search, including image search, local search, video search, academic search, news search and industry-specific vertical search engines. As an Internet marketing strategy, SEO considers how search engines work, what people search for, the actual search terms or keywords typed into search engines and which search engines are preferred by their targeted audience.

Optimizing a website may involve editing its content, HTML and associated coding to both increase its relevance to specific keywords and to remove barriers to the indexing activities of search engines. Promoting a site to increase the number of backlinks, or inbound links, is another SEO tactic.

SEO is not an appropriate strategy for every website, and other Internet marketing strategies can be more effective like paid advertising through PPC campaigns, depending on the site operator's goals. A successful Internet marketing campaign may also depend upon building high quality web pages to engage and persuade, setting up analytics programs to enable site owners to measure results, and improving a site's conversion rate. SEO may generate an adequate return on investment. However, search engines are not paid for organic search traffic, their algorithms change, and there are no guarantees of continued referrals. Due to this lack of guarantees and certainty, a business that relies heavily on search engine traffic can suffer major losses if the search engines stop sending visitors. Search engines can change their algorithms, impacting a website's placement, possibly resulting in a serious loss of traffic. It is considered wise business practice for website operators to liberate themselves from dependence on search engine traffic.

Search Engine Submission –

Search Engine Submission is how a webmaster submits a website directly to a search engine. While Search Engine Submission is often seen as a way to promote a web site, it generally is not necessary because the major search engines like Google, Yahoo, and Bing use crawlers, bots, and spiders that eventually would find most web sites on the Internet all by themselves. There are two basic reasons to submit a web site or web page to a search engine. The first reason would be to add an entirely new web site because the site operators would rather not wait for a search engine to discover them. The second reason is to have a web page or web site updated in the respective search engine. How web sites are submitted there are two basic methods still in use today that would allow a webmaster to submit their site to a search engine. They can either submit just one web page at a time, or they can submit their entire site at one time with a sitemap. However, all that a webmaster really needs to do is to submit just the home page of a web site. With just the home page, most search engines are able to crawl a site, provided that it is well designed. Most websites want to be listed in popular search engines, because that is how most people start their search for a product or service. A user seeks information on the web, using a search engine. Websites that appear on the first page of a search are, usually, called the top 10. Clicking on the blue URL / hyperlink causes the web page / website to appear in the web browser.

Thus, webmasters often highly desire that their sites appear in the top 10 in a search engine search. This is because searchers are not very likely to look over more than one page of search results, known as a SERPs. In order to obtain good placement on search

results in the various engines, webmasters must optimize their web pages. The process is called search engine optimization. Many variables come into play, such as the placement and density of desirable keywords, the hierarchy structure of web pages employed in a web site (i.e., How many clicks from the home page are required to access a particular web page?), and the number of web pages that link to a given web page. The Google search engine also uses a concept called page rank. PageRank relies on the uniquely democratic nature of the web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at considerably more than the sheer volume of votes, or links a page receives; for example, it also analyzes the page that casts the vote. Votes cast by pages that are themselves "important" weigh more heavily and help to make other pages "important." Using these and other factors, Google provides its views on pages' relative importance.

2.9 INTERNET MARKETING AND ITS E-CYCLE

Internet marketing, or online marketing, refers to advertising and marketing efforts that use the Web and email to drive direct sales via electronic commerce, in addition to sales leads from Web sites or emails. Internet marketing and online advertising efforts are typically used in conjunction with traditional types of advertising like radio, television, newspapers and magazines. Depending on whom you ask, the term Internet marketing can mean a variety of things. At one time, Internet marketing consisted mostly of having a website or placing banner ads on other websites. On the other end of the spectrum, there are loads of companies telling you that you can make a fortune overnight on the Internet and who try to sell you some form of "Internet marketing program". Today, Internet marketing, or online marketing, is evolving into a broader mix of components a company can use as a means of increasing sales - even if your business is done completely online, partly online, or completely offline. The decision to use Internet marketing as part of a company's overall marketing strategy is strictly up to the company of course, but as a rule, Internet marketing is becoming an increasingly important part of nearly every company's marketing mix. For some online businesses, it is the only form of marketing being practiced.

Internet Marketing Objectives

Essentially, Internet marketing is using the Internet to do one or more of the following:

- **Communicate a company's message** about itself, its products, or its services online.
- **Conduct research** as to the nature (demographics, preferences, and needs) of existing and potential customers.

- **Sell goods, services, or advertising space** over the Internet.

Internet Marketing Components

Components of Internet marketing (or online marketing) may include:

- **Setting up a website**, consisting of text, images and possibly audio and video elements used to convey the company's message online, to inform existing and potential customers of the features and benefits of the company's products and/or services. The website may or may not include the ability to capture leads from potential customers or directly sell a product or service online. Websites can be the Internet equivalents of offline brochures or mail order catalogs and they are a great way to establish your business identity.
- **Search Engine Marketing (SEM)**, which is marketing a website online via search engines, either by improving the site's natural (organic) ranking through search engine optimization (SEO), buying pay-per-click (PPC) ads or purchasing pay-for-inclusion (PFI) listings in website directories, which are similar to offline yellow page listings.
- **Email marketing**, which is a method of distributing information about a product or service or for soliciting feedback from customers about a product or service through Email. Email addresses of customers and prospective customers may be collected or purchased. Various methods are used, such as the regular distribution of newsletters or mass mailing of offers related to the company's product or services. Email marketing is essentially the online equivalent of direct mail marketing.
- **Banner advertising**, which is the placement of ads on a website for a fee. The offline equivalent of this form of online marketing would be traditional ads in newspapers or magazines.
- **Online press releases**, which involve placing a newsworthy story about a company, its website, its people, and/or its products/services with on online wire service.
- **Blog marketing**, which is the act of posting comments, expressing opinions or making announcements in a discussion forum and can be accomplished either by hosting your own blog or by posting comments and/or URLs in other blogs related to your product or service online.
- **Article marketing**, which involves writing articles related to your business and having them published online on syndicated article sites. These articles then have a tendency to spread around the Internet since the article services permit re-publication provided that all of the links in the article are maintained. Article marketing can result in a traffic boost for your website, and the distribution of

syndicated articles can promote your brand to a wide audience.

- **Social media marketing**, which can involve social networks like Twitter, LinkedIn, Facebook and social bookmarking sites like Digg.
- **Banner exchange** involves exchange of banner advertisements among websites that are useful and relevant to the particular websites. Both the parties exchanging banner advertisements earn revenues through their respective advertisement usages.
- **Shopping boots** are price comparison sites on the World Wide Web that automatically search the inventory of several different online merchants to find the lowest prices for consumers. Typically, these sites rank products by price and allow shoppers to link directly to an online merchant's site to actually make a purchase. Many shopping bots also include links to product reviews from evaluation sites.

2.10 PROS AND CONS OF ONLINE SHOPPING

The internet has made many things easier such as communicating with friends and family, banking etc. In these examples the internet saves time which in this day and age is a big convenience. The internet has allowed the development on online businesses which sell their products to a worldwide audience. Online businesses do not have overheads associated with a shop front meaning they often have lower prices than a traditional shop. However lower prices do not always mean you get the best value or that it is the most convenient shopping experience. As with most online activities, there are definite tradeoffs in online shopping between convenience, cost savings, choice, and privacy. Before you decide whether or not online shopping is for you, it is important to weigh the pros and cons of entering into the world of e-commerce

Pros of shopping online

- **Convenience** – One of the biggest benefits of online shopping is that you can buy almost anything you could imagine without ever leaving your house. Online stores are open 24 hours a day and are accessible from any location with an Internet connection.
- **Selection** – In general, online stores are able to carry more selection than traditional brick-and-mortar stores. Because online stores do not need to attractively display their items on shelves, they can keep a larger amount of inventory on hand. They also might only have small amounts of each item, since they do not need to display them, and can order more from their supplier as needed.
- **Information** – Online shops tend to provide more information about items for sale than you would get in a physical store. Product descriptions most often include a description from the manufacturer, another description from

the vendor, specific technical and size details, reviews from professional magazines and journals, and reviews from people who have bought the product. Online book stores often will have excerpts of the books (usually the first chapter) for you to read. Having all this information available when you are considering a purchase makes you a more informed consumer without having to perform extra research yourself.

- **Price** – Because online stores do not have to pay rent for a storefront in a nice part of town and tend to sell much larger quantities of goods, they can offer to sell products for a much lower price. Discounts online can be substantial—up to 25-50 percent off the suggested retail price. There are even some sites that only sell clearance items. However, buying online does take away from local business, so that is a consideration to keep in mind

Cons of shopping online

- **Hands-On Inspection** – One thing that online stores cannot replace is the experience of actually seeing and touching the item you are considering buying. For example, clothes shopping can be very tricky online, since you cannot try on the clothes before you buy. There may also be small details that you decide you do not like in a product that are not noticeable until you have it in your hand.
- **Shipping** – Some major online retailers now offer free shipping for their products, but many require you to meet a minimum order cost to qualify or only offer this incentive at certain times of year. In general, you should expect to pay an additional shipping cost on top of the price of the items that you order. For larger items, like furniture, this can really add up and becoming a major factor. Additionally, if you decide that you do not like a product, you will have to pack it back up and take it to the post office to return it. Again, some retailers will offer free returns, but some do require you to pay for return postage. In that case, even if you have decided against keeping an item, you have still had to pay several dollars for the shipping.
- **Wait Time** – Waiting for your item to arrive is another downside of online shopping. One of the great pleasures of shopping at a store is the instant gratification—you see something you like, you pay for it, and then you get to take it home and use it right away. In the case of online shopping, you may have to wait days or even weeks for the item to arrive at your door. Especially if you are in a time crunch, then you may want to consider purchasing your item at a local retailer.
- **Privacy** – When you shop online, you waive certain privacy rights to the online retailer. Online stores can track your purchases over time to give you more suggestions of things you might like to buy, send you e-mails with sale information, and, occasionally, sell your contact information

to other companies. These days, many brick-and-mortar stores do the same thing, tracking your information through your credit card (Target is a notable example). However, it is much trickier for traditional stores to do this, as you may sometimes pay in cash or refuse to provide your e-mail address at checkout. In contrast, by purchasing something in an online store, you sign away certain privacy rights—this is why it is always a good idea to read the Terms of Service.

CHECK YOUR PROGRESS

2. Fill in the blanks

(a) A _____ is responsible for maintaining the database of names registered within the TLD it administers.

(b) _____ employ a range of technologies to enable consumers to connect to their network.

(c) A _____ provider is a department or organization that provides email _____ hosting services.

(d) A _____ ISP is an operation which purchases services from another ISP.

(e) ____ ISPs are Internet service providers which provide _____ free of charge.

(f) Many techniques such as web content development, search engine optimization, and search engine submission, are used to increase a site's _____.

(g) _____ are specialized web site developers who have content generation skills such as graphic design, multimedia development, professional writing, and documentation.

(h) _____ is how a webmaster submits a _____ directly to a search engine.

(i) _____ businesses do not have overheads associated with a shop front.

(j) Waiting for your item to arrive is another downside of _____.

2.11 LET US SUM UP

- The ***Internet*** represents one of the most successful examples of the benefits of sustained investment.
- The ***World Wide Web*** is a system of interlinked hypertext documents accessed via the Internet.
- A ***domain name*** is an identification string that defines a realm of administrative autonomy, authority or control on the Internet.
- The right to use a domain name is delegated by ***domain name registrars.***
- An ***Internet service provider (ISP)*** provides services such as Internet access, Internet transit, domain name registration and hosting, dial-up access, leased line access.
- ***Website promotion*** is the continuing process used by webmasters to promote and bring more visitors to a website.
- ***Search engine optimization (SEO)*** is the process of affecting the visibility of a website or a web page in a search engine's "natural" search results.
- ***Internet marketing and online advertising*** efforts are used in conjunction with traditional types of advertising like radio, television, newspapers and magazines.

2.12 ANSWERS TO CHECK YOUR PROGRESS

1.
(a) Internet.
(b) web browsers, hyperlinks.

(c) URL, hyperlink.
(d) Domain Name System.
(e) Internet Protocol.

2.

(a) Registry.
(b) Access ISPs.
(c) mailbox, mailbox.
(d) virtual.
(e) Free, service.
(f) traffic.
(g) Content developers.
(h) Search engine submission, website.
(i) Online.
(j) online shopping.

2.13 FURTHER READINGS

1. E-Commerce Past, Present and Future by Karabi Bandyopadhyay, Vrinda Publications (P) Ltd., New Delhi, 2012
2. E-Commerce—Strategy, Technologies and Applications by David Whiteley,Tata McGraw—Hill Publishing Company Limited, New Delhi, 2006
3. E-Commerce Business, Technology, Society by Kenneth C. Laudon, and Carol Guercio Traver, Pearson Education, New Delhi, 2008

2.14 MODEL QUESTIONS

1. Write a brief note on the evolution of the internet.
2. What is a Domain name? Describe its purpose.
3. How do you register a Domain name? Explain.

4. Explain the term 'Web Promotion'. Discuss the different ways by which one can promote a website

5. Explain the concept of ISP and its importance in the context of the internet.
6. Explain the reasons involved in creating a website.

7. What do you mean by banner exchange and shopping boots

8. Explain the concept of Internet marketing.

9. What is online shopping? Explain its pros and cons.

UNIT 3: MOBILE COMMERCE

UNIT STRUCTURE

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to :

- define Mobile Commerce
- define Wireless Application Protocol(WAP)
- describe the technology behind WAP
- define and describe about Mobile Information Device
- describe applications of Mobile Computing

3.2 INTRODUCTION

We must aware of what technology is available in this information based global society that we live in. We must know the power of these new technologies and must know about how these technologies help us. By this time we have come across the overview of one of such technological application called E-commerce. We discussed there the advantages of using E-commerce and their applications in today's

developing world. From Unit 2, we have got the idea of the fastest growing segments of computer industry, which is about WWW and Internet. As the technology is emerging, new ideas and concepts are also coming everyday. One such type of web based emerging technology is the WAP technology and the result of this upcoming technology in this new era is the mobile commerce. This unit is giving the idea of this WAP technology as well as about the concept of the mobile commerce. Furthermore, in this unit we will also get the opportunity to leverage the power of the Mobile Information Devices (MID's) which is used to improve student learning and engagement.

3.3 MOBILE COMMERCE: DEFINITION

Mobile commerce or simply m-commerce is the amalgam of wireless personal digital assistants (PDAs) and network technology. It was originally coined by Kevin Duffey in 1997 with the idea to deliver electronic commerce capabilities directly into consumer's hand anywhere at any time via wireless technology. The hope was to use this idea mainly in banking and shopping. Now-a-days many mobile users made their purchase through their phones. The services available through m-commerce concept are:

- **Mobile money transfer**: Money can transfer through mobile to each other. The initiative first taken by a multimillion shillings company in Kenya.
- **Mobile ATM service**: Connecting mobile money platforms and provide bank grade ATM quality.
- **Mobile ticketing**: Tickets can be sent to mobile phones and users are then able to use their tickets immediately, by presenting their mobile phone at the ticket check. This technology can also be used for the distribution of vouchers, coupons, and loyalty cards.
- **Mobile Content purchase and delivery**: It mainly consists of the sale of ring-tones, wallpapers, and games for mobile

According to a survey in January 2013, 29% of mobile users have made a purchase with their mobile phones

phones. It is possible to purchase and delivery of full-length music tracks and video in mobile phone. The mobile with 4G networks make it possible to buy a movie on a mobile device in a couple of seconds.

- **Location-based services**: Through mobile it is possible to know some local information like Local discount offers, Local weather, Tracking and monitoring of people etc.

- **Information services**: A wide variety of services like news, sports scores, financial records, traffic reporting etc. are possible in mobile in the same way as it is delivered to PCs.

- **Mobile Banking or m-banking**: Allowing customers to access account information and make transactions, such as purchasing stocks, remitting money.

- **Mobile shopping**: Customers can shop online through mobile without having to be at their personal computer.

- Mobile marketing and advertising: Companies can advertise and campaign their product through mobile which get even better response than traditional campaigns.

3.4 WIRELESS APPLICATION PROTOCOL

Wireless Application Protocol (WAP) is a worldwide technical standard for accessing information over a mobile wireless network. The definition of each word separately means it as:

- **Wireless:** Lacking or not requiring a wire or wires pertaining to radio transmission.

- **Application:** A computer program or piece of computer software that is designed to do a specific task.

- **Protocol:** A set of technical rules about how information should be transmitted and received using computers.

3.5 WAP TECHNOLOGY

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones. A WAP device may be an enhanced mobile phone, PDA or notebook computer without any voice capability that uses wireless infrastructure. It has a WAP gateway to send and check web page requests. The first version of this service was WAP 1.0 which is later replaced by WAP 2.0 because of some problem arose in WAP 1.0. WAP is designed to scale across a broad range of wireless networks like GSM, IS-95, IS-136, and PDC.

To describe the technology behind WAP, we have to discuss first the protocol stack of it for accessing web that allowing interoperability of WAP equipment and software with different network technologies. The protocol stack is given in the following figure:

Figure 3.1 WAP protocol stack

Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)
Bearer Layer (GSM, CDMA, GPRS etc.)

The lowest layer supports all the existing mobile phone systems. Next is the WDP which is essentially a UDP. Security is needed in every wireless system which is done by WTLS. It provides a public-key cryptography-based security mechanism similar to TLS. Next is the transaction layer which manages all reliable or unreliable request and responses. WTP provides transaction support adapted to the wireless world. Then next is the session layer which is similar to HTTP/1.1. At the top of all is the microbrowser WAE. It uses Wireless Markup Language (WML). So a WAP device can access only those pages that have been converted to WML.

WAP Forum:

WAP forum is a group of companies in which joint effort the WAP technology has come into a reality. The objective of the forum is to create a license-free standard that brings information and telephony services to wireless devices. In December 1997, WAP Forum was formally formed and released the WAP 1.0 specifications in April 1998. After this, the companies like Motorola, Nokia, and Ericsson had taken up and tried to give advanced services in the wireless domain.

The WAP Forum now has over 500 members and represents over 95 percent of the global handset market. Companies such as Nokia, Motorola and Ericsson are all members of the forum.

WAP 2.0:

The first generation of WAP used circuit-switched network. As packet-switched network is always better, the next generation WAP 2.0 uses it. It is the re-engineered version of WAP 1.0 and was released in 2002. WAP 2.0 has some new features than WAP 1.0 like:

- Push and pull model
- Supporting telephone into applications
- Multimedia messaging
- Inclusion on 264 pictograms
- Interface to a storage device
- Support for plug-ins in the browser.

Because of the push model of WAP 2.0, data are arriving in mobile without being asked for. Data and voice are merged in WAP 2.0. It supports multimedia messaging. WAP 2.0 uses a cut-down version of XHTML with end-to-end HTTP by dropping the gateway and custom protocol suite. A WAP gateway is used as a standard proxy server. The role of WAP gateway is to shift from one of translation to adding additional information to each request. This is configured by the operator and includes telephone numbers, location, billing information, and handset information.

The two main technical differences present in WAP 2.0 technology are the protocol stack and the markup language. WAP 2.0

supports the old protocol stack that is given in figure 3.1 as well as new Internet stack with TCP and HTTP/1.1.

Figure 3.2 Protocol stacks of WAP 1.0 and WAP 2.0

XHTML	
WSP	HTTP
WTP	TLS
WTLS	TCP
WDP	IP
Bearer Layer	Bearer Layer
WAP 1.0 Protocol Stack	WAP 2.0 Protocol Stack

WAP 2.0 supports both the given protocol stacks. However, some minor changes to TCP were made here. Those are:

- It uses fixed 64 KB windows
- No slow start
- Maximum MTU of 1500 bytes
- Different re-transmission algorithm

Why is WAP important?

Before emerging the WAP technology, the Internet facility was limited to only computers. But now because of WAP devices it is possible to get massive information, communication, and data resources of the Internet more easily with a mobile phone or communications device for anyone.

WAP being open and secure, is well suited for many different including applications, but not limited to stock market information, weather forecasts, enterprise data, and games. The current set of web application development tools will easily support WAP development, and in the future more development tools will be announced.

WAP Microbrowser

As we need a browser to browse any standard internet site, in the same way to browse a WAP enables website, a micro browser is needed. It is a small piece of software that makes minimal demands on hardware, memory and CPU. It can display information written in a restricted mark-up language called WML. Although, tiny in memory footprint it supports many features and is even scriptable.

Today, all the WAP enabled mobile phones or PDAs are equipped with these micro browsers. Because of this, we can get full advantage of WAP technology in our mobile phones and in other wireless devices.

CHECK YOUR PROGRESS 1

1. Fill in the blanks

a) PDAs are _____ network technology.

b) Mobile commerce is the mixture of wireless PDAs and _____.

c) Mobile money transfer facility was introduced first in _____.

d) WAP 2.0 has both _____ and _____ model.

e) WAP 2.0 has the _____ facility.

2. Write True or False

a) Micro browser is needed to browse any WAP enables website,

b) WAP 1.0 support HTTP/1.1 in their protocol stack.

c) WAP 2.0 supports the old protocol stack and new Internet stack with TCP and HTTP/1.1.

d) Mobile commerce was originally coined to deliver electronic commerce capabilities directly into consumer's hand anywhere at any time via wireless technology.

e) WAP 1.0 has feature of Push and pull model

3.6 MOBILE INFORMATION DEVICE

Mobile Information Device is a device which can improve student learning process. It can engage anyone for long. This is basically a mobile computer with which we can anticipate a successful learning environment. Mobile information devices are the wireless information devices that include PDAs, Notebooks, IPads, Tablets, Digital Cameras, Recording Devices, Laptop computers, Cell phones, Smart phones, GPS devices etc. Early pocket sized devices are connected with modern computers in late 2000s. In PDA, the input and output of modern mobile devices are combined into touch screen interface. Smartphones and PDAs are popular among all conventional computing devices. Enterprise digital assistants are extend to avail the functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Recent devices employ handheld devices that combine video, audio and on-screen drawing capabilities. Because of these facilities now it is enabling for user to participate in multi-party conference in real-time, independent of location. Users can watch television through Internet on mobile devices. Today's devices have been designed together for many applications like mobile computers, digital still cameras, digital video cameras, mobile phone, pager, personal navigation device etc.

We are very much familiar of our mobile devices which are also a part of the mobile information device, are a small, handheld computing device. It has a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg). Nokia, HTC, LG, Motorola Mobility, BlackBerry, and Apple are just a few examples of the many manufacturers that produce these types of devices.

Each mobile information devices have an operating system (OS) and application software to operate on. Most of MIDs have Wi-Fi, Bluetooth, and GPS capabilities facility to connect to the Internet and other Bluetooth-capable devices. Smart phones and PDAs are very popular devices that have power of a conventional computer in environments.

Uses

Mobile Information Devices are to be used in a way to positively support:

- Instruction
- Integrity of any learning environment or assessment situation
- Child Internet Protection Act
- Mobile technology etiquette

The uses of mobile information devices include:

- digitizing notes
- sending and receiving invoices
- asset management
- recording signatures
- managing parts
- scanning barcodes.

Overall, MIDs are used to support learning during instructional times, at the direction of the learner.

Characteristics

The characteristics are:

- Portability: Can function and operate consistently while moving. They contain rechargeable batteries that allow several hours or more of operation without access to an external charger or power source.

- Smaller in size: Because of its small size, the user can operate in one hand, and can hold very easily while moving.

- Wireless communication: Wireless makes these devices more usable and handy.

Benefits

The benefits of MIDs are:

- Help in preparing students to meet the 21st Century Information Based Global Society
- Mobile Device Etiquette that increases the good manner
- Decrease in Referrals
- Cost Savings due to less price than earlier personal computers
- Information Gathering – Student / staff surveys information via MIDs.
- Improving teaching-learning process, because MIDs make this process easier to demonstrate.

Features

The features of MIDs are the set of capabilities, services and applications that they offer to their users. Low-end mobile phones are often referred to as feature phones, and offer basic telephony. Though manufacturer wise MIDs have different features, there are some common components. They are:

- A battery that providing the power source
- An input mechanism to allow the user to interact with the phone. The most common input mechanism is a keypad and touch screens.
- In most of the MIDs have the basic mobile phone services to allow users to make calls and send text messages.
- Roaming facility
- WAP services

- Bluetooth facility

3.7 MOBILE COMPUTING APPLICATIONS

Before going directly to the computing applications, we have to know what is mobile computing. It is basically the human-computer interaction. It is a type of computing which use Internet and cell phones. It is used to mean a wide range of consumer electronics. Digital cameras and standard MP3 players are considered as mobile computing devices.

The process of mobile computing involves mobile communication, mobile hardware and mobile software. Here, Communication includes ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.

Applications are applicable mainly for the:

- Emergency services
- Stock information collation or control
- Credit card verification
- For estate agent
- Vehicle dispatch
- Electronic mail or paging
- Transmission of news
- Information about road condition
- Internet access
- intelligent travel guide with up-to-date location dependent information
- direct access to central customer files
- local environmental related news and
- Entertainment like multi user games, movies, music etc.

CHECK YOUR PROGRESS 2

3. Fill in the blanks

a) _____ is a mobile computer with which we can anticipate a successful learning environment.

b) Mobile information devices are the _____ information devices.

c) In PDA, the input and output of modern mobile devices are combined into _____.

d) _____ is basically the human-computer interaction.

e) _____ deals with the characteristics and requirements of mobile applications.

4. Write True or False

a. Information can gather by any student or staff via MIDs.

b. Because of MIDs demonstrating facilities one can improve the teaching-learning process.

c. MID does not allow the user to interact with the phone.

d. MIDs are bigger in size.

e. Hardware of mobile computing includes mobile devices.

3.8 LET US SUM UP

From this unit we have acquired the ides of new emerging technology which is basically the wireless communication technology. We got the concept of this technology which captures in every steps of day to day life and makes the life modern very fast.

First of all this unit describes the idea of Mobile commerce. We also called it as m-commerce. It is the mixture of wireless personal digital assistants (PDAs) and network technology. The idea behind m-commerce is to deliver electronic commerce capabilities directly into consumer's hand anywhere at any time via wireless technology. This concept grasp today's market basically in banking and shopping. We can now purchase anything through our mobile phones whenever required. Mobile money transfer, Mobile ATM service, Mobile ticketing are some familiar examples of m-commerce.

To access information worldwide in this wireless technology, there should be some standard rules which are known as Wireless Application Protocol (WAP). This is the standard of rules that is used to transmit and receive information using computers. The WAP is a result of joint efforts taken by companies teaming up in an industry group called WAP Forum. In December 1997, WAP Forum was formally created and released WAP 1.0 specifications in April 1998.

If we think of the technology behind WAP, the WAP 1.0 used circuit-switched network and WAP 2.0 packet-switched network which is always better. WAP 2.0 is the re-engineered version of WAP 1.0 and was released in 2002. The two main technical differences between WAP 1.0 and WAP 2.0 technology are the protocol stack and the markup language. The differences of protocol stack are clearly given in the figure 3.2. WAP 2.0 supports the protocol stack of WAP1.0 as well as the new Internet stack with TCP and HTTP/1.1.

Next section describes about the mobile information devices. It is a wireless information device. PDAs, Notebooks, IPads, Tablets, Digital Cameras, Recording Devices, Laptop computers, Cell phones, Smart phones, and GPS devices are some example of it. Recent development of these devices improves the teaching-learning process; it can engage anyone for long. Recent devices employ handheld devices that combine video, audio and on-screen drawing capabilities. We have got many facilities from this development. Tele-conferencing, mobile-shopping, mobile learning, e-ticketing are became easier now-a-days due to the development of mobile information devices.

3.9 ANSWERS TO CHECK YOUR PROGRESS

1. a) wireless b) network technology c) Kenya d) Push, pull e) packet-switched

2. a) Trueb) False c) True d)True e) False

3. a) mobile information device b) wireless
   c) touch screen interface d) mobile computing
   e) Mobile Software

4. a) True b)True c) False d) False e) True

3.10 FURTHER READING

1. Tanenbaum A.S. C*omputer Network*, Prentice Hall, India.
2. "A brief History of WAP". *HCI blog*. December 8, 2004.
3. B'Far R. (2004). *Mobile Computing Principles: Designing and Developing Mobile Applications with UML and XML*. Cambridge University Press.
4. Poslad S. (2009). *Ubiquitous Computing: Smart Devices, Environments and Interactions*. Wiley.
5. Rhoton J. (2001). *The Wireless Internet Explained*. Digital Press.
6. Talukder A., Yavagal R. (2006). *Mobile Computing: Technology, Applications, and Service Creation*. McGraw-Hill Professional.

3.11 MODEL QUESTIONS

1. What is mobile commerce? Write the services available in mobile commerce.
2. What do you mean by location-based service and information service?
3. Define WAP. Write the technology behind it.

4. Write the differences between original WAP and later WAP. Show their protocol stack.
5. Why WAP is important. Write the uses of it.
6. Define WAP microbrowser. Describe WAP 2.0 technology.
7. What do you mean by Mobile information devices? Write few examples of it.
8. Write the characteristics and uses of mobile information devices.
9. Why mobile information device is important? Write its benefits.
10. What is mobile computing? Discuss its applications.

*****

UNIT 4: WEB SECURITY

UNIT STRUCTURE

4.1 LEARNING OBJECTIVES

After going through this unit, you will able to :

- learn about the key issues in web security
- learn how information is protected from unauthorized interception during transaction
- describe privacy control over one's personal data
- define corporate policy on e-mail privacy
- explain security threats on computer system and the various

packages available for security

- get an idea about hacking
- learn about computer viruses , how it spreads and protection from viruses
- learn about firewall, its component, importance, design issues and limitations

4.2 INTRODUCTION

Web security is a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organizations. Security protects you against unexpected behavior. Securing Internet commerce is probably the biggest challenge that web security professionals have yet faced. Few years ago, Internet commerce did not exist. Today it is attracting enormous financial interest. Investors are enthusiastically backing companies that promise to deliver the hardware and software which Internet commerce requires. Companies are investing in purchases of hardware and software to permit them to engage in Internet commerce.

One important question is that why should web security require special attention apart from the general subject of computer and Internet security? Because the Web is changing many of the assumptions that people have historically made about computer security and publishing:

The Internet is a two-way network. As the Internet makes it possible for web servers to publish information to millions of users, it also makes it possible for computer hackers, crackers, criminals, vandals, and other "bad guys" to break into the very computers on which the web servers are running. Those risks don't exist in most other publishing environments, such as newspapers, magazines, or even "electronic" publishing systems involving teletext, voice-response, and fax-back.

The World Wide Web is increasingly being used by corporations

and governments to distribute important information and conduct business transactions. Reputations can be damaged and money can be lost if web servers are subverted. Although the Web is easy to use, web servers and browsers are exceedingly complicated pieces of software, with many potential security flaws. Many times in the past, new features have been added without proper attention being paid to their security impact. Thus, properly installed software may still pose security threats. Once subverted, web browsers and servers can be used by attackers as a launching point for conducting further attacks against users and organizations.

Unsophisticated users will be common users of www-based services. The current generation of software calls upon users to make security-relevant decisions on a daily basis, yet users are not given enough information to make informed choices.

4.3 SECURITY ISSUES ON WEB

The security problems affecting the three areas of Internet commerce are summarized in the following three sections.

Credit Card Transactions

There is considerable, and justifiable, fear that confidential information, such as credit cards and personal details, could be intercepted during transmission over the Internet, for example when submitting an order form on the Web. The challenge is to transmit and receive information over the Internet while insuring that:

* it is inaccessible to anyone but sender and receiver (privacy),
* it has not been changed during transmission (integrity),
* the receiver can be sure it came from the sender (authenticity),
* the sender can be sure the receiver is genuine (non-fabrication),
* the sender cannot deny he or she sent it (non-repudiation)

Without special software, all Internet traffic travels "in the clear" and so anyone who monitors traffic can read it. This form of "attack" is relatively easy to perpetrate using freely available "packet sniffing" software since the Internet has traditional been a very "open" network. If you use the "trace route" command from a Unix workstation

that is communicating across the Internet you can see how many different systems the data passes through on the way from client to server. At the beginning and end of the list you will probably see "local providers" or ISPs(Internet Service Providers). Most of these are considered "easy targets" by hackers, particularly if the ISP has servers on a college campus. In between you will probably see several machines operated by big name communications providers, such as Sprint or MCI. These may be more secure, but illegal penetration of even these systems poses "no problem" to some hackers.

Typically, a sniffing attack proceeds by compromising a local ISP at one end of the transmission. No special physical access is required (it is also possible to eavesdrop using network diagnostic hardware if you have physical access to the network cabling). Passwords and credit cards can be distinguished from the rest of the traffic using simple pattern matching algorithms. The defense against this type of attack is to encrypt the traffic, or at least that portion which contains the sensitive data. However, encryption incurs performance overhead and requires coordination between legitimate parties to the communication. In commercial terms, such coordination requires widespread standards for secured transactions, which have been slow to emerge. Note that protecting transactions is only one element of the secure transaction problem. Once confidential information has been received from a client it must be protected on the server. Currently, Web servers are among the softest targets for hackers, largely due to the immaturity of the technology.

Virtual Private Networks

This is a specialized form of encrypted Internet transaction allowing a secure channel or tunnel to be established between two systems for the purposes of electronic data interchange. This differs from credit card and consumer ordering transactions in that the volume of data between the two parties is greater and the two parties are well known to each other. This means that complex and proprietary encryption

and authentication techniques can be used since there is no pretense to offer universal connectivity through this channel. Despite the potential for greater security, the VPN is still a worrying development from a security perspective. For a start there is the attention that this "increased security" will attract from hackers and possibly leading to embarrassing or even costly cracking of codes. However, even if the encryption techniques employed by the digital tunneling systems currently on the market or under development prove to be very powerful, thus insuring confidentiality and availability of data, this still leaves the third aspect of security, availability. There are currently hundreds of retail operations that depend upon just-in-time inventory replacement. The data that triggers the delivery from the manufacturer travels electronically from the store, currently over private lines. If public lines, i.e. the Internet, are used, the potential for intentional disruption is enormous, not to mention the current lack of protection against accidental service outages.

Digital Certification

This area will continue to grow in importance as companies seek trusted third parties to hold digital certificates that can be used to electronically prove the identities of message senders and receivers, the integrity of documents (e.g. that an invoice has not been changed) and even the validity of digital media, such as sound recordings, photographs, and so on (e.g. if crime scene photographers switch to digital cameras someone will need to verify that the images presented in court as the same as those originally taken at the scene). While the cryptographic basis of these mechanisms is impressive, they leave open several possible areas of exploitation in terms of sharp practice, fraud, extortion, and so on. It is not fanciful to imagine the value of digital certificates reaching a point where the temptation to betray trust, which rests upon less-than-perfect humans, will be considerable.

4.4 Secure Transaction

Much of the attention that has been paid to web security has involved the problem of protecting information from unauthorized interception as it travels over the Internet.
There are many ways to protect information from eavesdropping as it travels through a network: Physically secure the network, so that eavesdropping is impossible. Hide the information that you wish to secure within information that appears innocuous. Encrypt the information so that it cannot be decoded by any party who is not in possession of the proper key.Of these techniques, encryption is the only one that is practical. Physically securing the Internet is impossible. Information hiding only works if the people you are hiding it from do not know how it is hidden.

One of Netscape Communication's early innovations was its Secure Socket Layer (SSL), a system for automatically encrypting information as it is sent over the Internet and decrypting it before it is used.

SSL is an important part of web security, but it is only one component. Ironically, even though SSL was originally developed to allow the transmission of information such as credit card numbers over the Internet, new protocols may allow those kinds of financially oriented transmissions to be conducted more simply and more securely. Meanwhile, technologies such as digital certificates are eliminating the need to use SSL's cryptographic channel for sending usernames and passwords. The real promise of SSL, then, may be for providing secure administrative access to web servers and for allowing businesses to transmit proprietary information over public networks.

Current implementations of SSL in the U.S. provide two levels of security: export-grade and domestic. These two levels are a direct result of U.S. government restrictions on the export of cryptographic technology. Export-grade security protects data against casual eavesdropping, but cannot resist a determined attack. For instance, a rela-

tive novice with a single Pentium computer can forcibly decrypt an export-grade SSL message in less than one year using a brute force search (trying every possible encryption key). Domestic-grade security is much stronger: for practical purposes, messages encrypted with SSL's typical domestic-grade encryption should resist brute force attempts at decryption for at least 10 years, and should possibly be secure for 30 years or longer. Unfortunately, most versions of Netscape Navigator in circulation provide only for export-grade security, not domestic.

Another risk to information in transit is a denial-of-service attack resulting from a disruption in the network. A denial of service can result from a physical event, such as a fiber cut, or a logical event, such as a bug in the Internet routing tables. Or it can result from a sustained attack against your servers from attackers on the Internet: the attacker might try bombarding your web server with thousands of requests every second, preventing legitimate requests from getting through.

Today there is no practical way to defend against denial-of-service attacks, although redundancy and backup systems can help to minimize their impact. Ultimately, it will take effective use of the legal system to pursue and prosecute attackers to make these attacks less frequent.

4.5 COMPUTER MONITORING

Aside from obvious criminal activities, subtler forms of computer activity can pose ethical problems. For instance, the use of company computer equipment by employees for personal activities has been vigorously debated, but no clear answers have been formulated that can apply in all organizations. Most employees that use computers maintain an e-mail account and regularly check their mail at work. Generally, this is essential since internal company communications often are transmitted via e-mail. However, employees also may re-

ceive personal e-mail at the same account and spend their time at work using the company computer to send and receive personal messages.

New technologies not only allowed for the monitoring of e-mail communications, but other Internet activity such as listservs, chat rooms, and even Web browsing. While companies may well wish to make sure their employees are using their time for company purposes, the monitoring of Web traffic strikes many as an ethical lapse, particularly since the reasoning behind visiting a Web site cannot be determined simply by knowing that an individual went there. This problem extended far beyond the company setting. Fears over governmental or private monitoring of individuals' activities on the Internet opens up an entire range of serious ethical concerns. Because the context of a certain kind of communication or site visitation may be unknown to outside monitors, there is a significant possibility of misunderstanding, misinterpretation, and misuse of such acquired data.

The conflict between personal privacy and company surveillance of e-mail communications and other computer activity was one of the most widely publicized computer-ethical controversies in the late 1990s and early 2000s. While companies argue that the monitoring of their own systems to ensure their appropriate use and the beneficial use of company time is necessary to maintain competitiveness, the moral right to personal privacy was continually asserted.

4.6 PRIVACY ON INTERNET

Privacy is the control over one’s personal data and security ,the attempted access to data by unauthorized others – are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both.

Privacy is a serious issue in electronic commerce, no matter what source one examines. Forty-one percent of Web buyers surveyed

last year by Forrester Research of Cambridge, Mass., said they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely. ." A Business Week/ Harris Poll found that over forty percent of online shoppers were very concerned over the use of personal information, and 57% wanted some sort of laws regulating how personal information is collected and used. Similarly, privacy concerns were a critical reason why people do not go online and provide false information online. The majority of online businesses "had failed to adopt even the most fundamental elements of fair information practices. Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses. The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce.

Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity. An individual's privacy, as such, is always in an inherent state of tension, since it must be defined in conjunction with capabilities of others to transact business and even to control their own privacy. Privacy may have to be traded off in certain transactions, such as the access to credit or to maintain the quality of health care. Indeed, societal needs may also transcend an individual's privacy concerns, as in the case of public health. Nonetheless, individuals as e-commerce consumers, even with its inherent tradeoffs, still wish to control their personal information. Besides "privacy", a number of terms -- such as notice, choice, identification, digital persona, authentication, anonymity, pseudonymity and trust -- are used in privacy discussions.

4.7 CORPORATE EMAIL PRIVACY

Consider a small example, the company accountant accidentally sent some sensitive information to everyone in the office instead of just

the corporate officers because the Reply to All button was selected instead of simply Reply. An honest mistake, to say the least, but one with potentially serious consequences. The question that can be asked is if it could be unsent, and simply intercept the e-mails before they were downloaded by the users' Outlook.

In this particular case, the company in question clearly makes it known in written office policy documentation that when it comes to e-mail generated on and received by company computers, on company time, and using company resources, there should be no expectation of privacy, and any e-mail is subject to review.

The reason for this policy is two-fold. First, it's not to snoop but rather to ensure anyone's project could be addressed by another person should the need arise. Nobody is in the office 100 percent of the time, and cases will come up when a person's e-mail will have to be accessed for some reason or another. The second reason, of course, is to make it perfectly clear that these are company resources, that personal activity should be kept to a minimum, and that the company reserves the right to access that e-mail account. Some companies may not have such a written policy, but in the absence of such, it might be an unspoken policy.

4.8 SECURITY THREATS AND ATTACK ON COMPUTER SYSTEM

Security is the soft white underbelly of broadband Internet service and the threats are real. How pervasive are security threats on the Internet?

· The 2000 Computer Crime and Security Survey published by the FBI and Computer Security Institute found that 71% of all companies reported being attacked by independent external hackers in the last 12 months.

· According to IDC, the average new DSL connection experiences

three attempted “hacks” in the first 48 hours.
Security threats come in a variety of forms, but the results are the same: a serious disruption to business. Common types of Internet security threats are :

1. **Unauthorized Access to Your Network**. Hackers breaking into your network can view, alter, or destroy private files. A hacker can, for example, modify accounting, medical, or academic records, and then leave, with the break-in and changes going undetected until it is too late. Hackers may use a variety of readily available “hacker’s helper” tools to break into the network. Once in, the hacker has control of your computer and access to your confidential data.

2. **Denial of Service (DoS) Attacks**. Increasingly prevalent Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood and LAND Attack, aim not to steal information, but to disable a device or network so users no longer have access to network resources. Even if your network is not being attacked, it can be used as an unwitting ally in Denial of Service attacks on other networks. Using Trojan Horses or other malicious attachments, hackers plant tools on hundreds and sometimes thousands of computers to be used in future attacks. So, in addition to protecting your own LAN from attacks, you need to prevent your LAN computers from being compromised and used in attacks on others.

3. **Viruses**. These are destructive programs that attach themselves to E-mail, applications and files. Once on your LAN computers, viruses can damage data or cause computer crashes. Users can quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses. Viruses can also be used as delivery mechanisms for hacking tools, putting the security of the organization in doubt, even if a firewall is installed.

4. **Capture of Private Data Going Over the Internet**. As your private data moves over the Internet, hackers using programs called packet sniffers can capture your data as it passes from your network

over the Internet and convert it into a readable format. The source and destination users of this information never even know that their confidential information has been tapped.

5. Password-Based Attacks. A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to your network with a valid account, an attacker can do any of the following: Obtain lists of valid user and computer names and network information.Modify server and network configurations, including access controls and routing tables. Modify, reroute, or delete your data.

6. **Offensive Content**. Inappropriate Internet content can create an uncomfortable work environment and cause potential legal problems for your business. Network users risk viewing inappropriate content, decreasing productivity, and inviting lawsuits by abusing company resources with unregulated Web browsing.

CHECK YOUR PROGRESS-1

1. An attempt to make a computer resource unavailable to its intended users is called

a) denial-of-service attack b) virus attack

c) worms attack d) botnet process

2. The primary goal of the ……. protocol is to provide a private channel between communicating application, which ensures privacy of data authentication of the partners, and integrity.

a) SSL b) ESP

c) TSL d) PSL

3. The primary choice for password storage:

a) Clear text b) Encrypted password

c) Hash value of a password d) All of the above

4. The best storage locations for passwords is.

a) A-Root or administrator readable only

b) Readable by anyone.

c) Any file

d) All of the above.

5. A(n) _____ is a pseudo private data network that uses public bandwidth in combination with a tunneling protocol and security procedures.

a) value added network (VAN)

b) intranet

c) virtual private network

d) leased line

6. Characteristics of Trusted Software are:
a) Functional Correctness
b) Enforcement of Integrity
c) Limited Privilege
d) all

4.9 Software Packages for Privacy

Privacy software is software built to protect the privacy of its users. The software typically works in conjunction with Internet usage to control or limit the amount of information made available to third-parties. The software can apply encryption or filtering of various kinds.

Privacy software can refer to two different types of protection. One type is protecting a user's Internet privacy from the World Wide Web. There are software products that will mask or hide a user's IP address from the outside world in order to protect the user from identity theft. The second type of protection is hiding or deleting the users Internet traces that are left on their PC after they have been surfing the Internet. There is software that will erase all the users Internet traces and there is software that will hide and encrypt a user's traces so that others using their PC will not know where they have been surfing.

Some software packages used for privacy are :

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

GNU Privacy Guard (GnuPG or GPG) is a GPL Licensed alternative to the PGP suite of cryptographic software. GnuPG is a hybrid encryption software program in that it uses a combination of

conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is only used once.

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively.

Mozilla Firefox, Portable Edition is a repackaged version of Mozilla Firefox created by John T. Haller. The application allows Firefox to be run from a USB flash drive, CD-ROM, or other portable device on any Windows computer or Linux/UNIX computer running Wine. The program does not require Firefox to be installed on the computer, nor does it leave personal information on the computer or interfere with any installed versions of Firefox, though installation on a hard drive is possible.

4.10 Hacking

During the 1990s, the term "hacker" originally denoted a skilled programmer proficient in machine code and computer operating systems. In particular, these individuals could always hack on an unsatisfactory system to solve problems and engage in a little software company espionage by interpreting a competitor's code.

Unfortunately, some of these hackers also became experts at accessing password-protected computers, files, and networks and came to known as "crackers." Of course, an effective and dangerous "cracker" must be a good hacker and the terms became intertwined. Hacker won out in popular use and in the media and today

refers to anyone who performs some form of computer sabotage.

There now are more than 100,000 known viruses with more appearing virtually daily. The myriad of hackers and their nefarious deeds can affect any computer owner whether an occasional home user, e-mailer, student, blogger, or a network administrator on site or on the internet. No matter your level of computer use, you must protect your computer, business, or even your identity. The best way to know how to protect your computer is to understand the hacker's tools and recognize their damage.

4.11 Computer Virus

A computer virus is a small software program that spreads from one computer to another and interferes with computer operation. A computer virus might corrupt or delete data on a computer, use an email program to spread the virus to other computers, or even delete everything on the hard disk.

For example, the Melissa virus in March 1999 was spectacular in its attack. Melissa spread in Microsoft Word documents sent via e-mail, and it worked like this:
Someone created the virus as a Word document and uploaded it to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document, thinking it was harmless. The virus would then create 50 new messages from the recipient's machine. At that rate, the Melissa virus quickly became the fastest-spreading virus anyone had seen at the time. It forced a number of large companies to shut down their e-mail systems to control the spread.
The ILOVEYOU virus, which appeared on May 4, 2000, was even simpler. It contained a piece of code as an attachment. People who

double-clicked on the attachment launched the code. It then sent copies of itself to everyone in the victim's address book and started corrupting files on the victim's machine. This is as simple as a virus can get. It is really more of a Trojan horse distributed by e-mail than it is a virus.

Computer viruses usually spread in one of three ways: from removable media; from downloads off the Internet; and from e-mail attachments.

Although the Internet gets a bad rap as a source of viruses, you're no more likely to contract a virus from the Web than you are from packaged software. Still, scan everything you download, and update your antivirus software regularly.
E-mail is not the virus breeding ground it's made out to be, either. In fact, it's nearly impossible for a virus to be transmitted by plain-text e-mail. Most viruses can only spread via attachments — either rich-text e-mail or attached applications. Using antivirus software, scan attachments from people you know, and never open attachments from people you don't. If you're a Microsoft Outlook user, you can also select security preferences that keep e-mail-borne viruses from exploiting the close relationship between Outlook and the Windows operating system.

Protecting Computer

Install only trusted software and delete unknown emails. If you have any doubt about a piece of software's function, do not install it. If you receive e-mails from random people's names, resist your curiosity and do not open it, just delete it.

Under no conditions download or open attachments from anyone that you do not know and even then be cautious. Banks and most companies that create online personal accounts will not send you attachments. If they do, it is probably best to go to the company site and request the download or at least see if it is legitimate.

Whether in your e-mail or online, do not click on ads. If the ad is of interest, find the site. Be careful with what you physically put into your computer. This is especially true for shared R/W CDs, USB hard disks, or flash drives. This is an easy path for a virus to follow from computer to computer.

Protection: Install Anti-Virus Software

Anti-virus software searches for evidence of the presence of viral programs, worm, bombs, and Trojan horses by checking for the characteristic appearances or behaviors that is typical of these programs. When found the program logs its discovery, its type, often its name or an identifier, and it potential for damage. The anti-virus software then eliminates or isolates/quarantines the infected files. For the individual, commercial software is relatively inexpensive; however, there are free anti-virus programs available.

Since new viruses appear almost daily with new code it is imperative that you update you antivirus program often to keep up with these threats; therefore, make sure to set your program to update automatically. To avoid the annoyance of computer slowdown schedule full scale scans late at night.

The same is true for your Windows Operating System. Very often, your OS is where hackers discover the holes to exploit. Of course, in an ever-continuing battle, this software is continuously updated with security patches.

Finally, secure your wireless network with a router that has a built in firewall. Almost all wireless routers are set to no security when first installed. Log into the router and at least set it to basic security with a strong password to replace the factory setting that any hacker knows. A firewall or router that is not configured properly or non-existent allows hackers to scan passwords, e-mails, or files that cross your network connection.

4.12 Importance of Firewall

An Internet firewall is a device that is designed to protect your computer from data and viruses that you do not want. A firewall is so called because of the real firewalls used to secure buildings. A physical firewall is a set of doors that closes in a building so as to contain a fire to one area, preventing the entire building from being destroyed. Likewise an Internet firewall is designed to shut off access to your operating system or to other computers that are connected to your network.

A firewall is something that the user of the computer is responsible for checking and installing. The security levels provided by the firewall can be altered just as any other control function can be altered. Security experts say that the best way to stay safe online is to only visit websites that you trust or that you are sure are secure. In cases like these where the visiting of only a few sites is taking place, a firewall is still useful but does not have to work as hard to filter out dangerous content.

However, most Internet users visit more sites than just those that they are familiar with. In fact, many people use the Internet to do business, to research topics, to shop, to meet new people, etc. This typical Internet use is what really makes having an Internet firewall important. With a good Internet firewall, you are being protected from the spread of hacker dangers, many times without even being aware of it.

An Internet firewall is important for many reasons. Some value a firewall for its ability to keep private information secure. Identity theft is a growing crime and many see firewalls as a good defense against these specific types of predators. Others, such as small business owners, think firewalls are important because a firewall keeps all their personal electronic information private. Not only is privacy important from a competitive perspective, but you must make certain that you

can assure your customers that their personal business information is going to be safe with you.

Make sure that the information on your computer and the information that you share online remains for your eyes only. Take advantage of firewall protection and the fact that it comes standard with newer computers and can often be downloaded for free from a reputable site. No matter how you connect to the Internet an Internet firewall is important. Protect yourself, your business and your colleagues on your network by making sure that you have firewall protection.

4.13 Components of Firewall

The primary components of a firewall are:
a) Network policy,
b) Advanced authentication mechanisms,
c) Packet filtering, and
d) Application gateways.

Network Policy
There are two levels of network policy that directly influence the design, installation and use of a firewall system. The higher-level policy is an issue-specific, network access policy that defines those services that will be allowed or explicitly denied from the restricted network, how these services will be used, and the conditions for exceptions to this policy. The lower-level policy describes how the firewall will actually go about restricting the access and filtering the services that were defined in the higher level policy

Advanced authentication mechanisms
For years, users have been advised to choose passwords that would be difficult to guess and to not reveal their passwords. However, even if users follow this advice (and many do not), the fact that intruders can and do monitor the Internet for passwords that are transmitted in the clear has rendered traditional passwords obsolete. Advanced au-

thentication measures such as smartcards, authentication tokens, biometrics, and software-based mechanisms are designed to counter the weaknesses of traditional passwords. While the authentication techniques vary, they are similar in that the passwords generated by advanced authentication devices cannot be reused by an attacker who has monitored a connection. Given the inherent problems with passwords on the Internet, an Internet-accessible firewall that does not use or does not contain the hooks to use advanced authentication makes little sense.

Packet filtering

Filtering can be used in a variety of ways to block connections from or to specific hosts or networks, and to block connections to specific ports. A site might wish to block connections from certain addresses, such as from hosts or sites that it considers to be hostile or untrustworthy. Alternatively, a site may wish to block connections from all addresses external to the site with certain exceptions, such as with SMTP for receiving e-mail. Adding TCP or UDP port filtering to IP address filtering results in a great deal of flexibility.

Application Gateways

To counter some of the weaknesses associated with packet filtering routers, firewalls need to use software applications to forward and filter connections for services such as TELNET and FTP. Such an application is referred to as a proxy service, while the host running the proxy service is referred to as an application gateway. Application gateways and packet filtering routers can be combined to provide higher levels of security and flexibility than if either were used alone.

As an example, consider a site that blocks all incoming TELNET and FTP connections using a packet filtering router. The router allows TELNET and FTP packets to go to one host only, the TELNET/FTP

application gateway. A user who wishes to connect inbound to a site system would have to connect first to the application gateway, and then to the destination host.
Proxy services allow only those services through for which there is a proxy. In other words, if an application gateway contains proxies for FTP and TELNET, then only FTP and TELNET may be allowed into the protected subnet, and all other services are completely blocked. For some sites, this degree of security is important, as it guarantees that only those services that are deemed ``trustworthy'' are allowed through the firewall. It also prevents other untrusted services from being implemented behind the backs of the firewall administrators.

Another benefit to using proxy services is that the protocol can be filtered. Some firewalls, for example, can filter FTP connections and deny use of the FTP put command, which is useful if one wants to guarantee that users cannot write to, say, an anonymous FTP server.

4.14 Factors to consider Firewall design

The firewall design policy is specific to the firewall. It defines the rules used to implement the service access policy. One cannot design this policy in a vacuum isolated from understanding issues such as firewall capabilities and limitations, and threats and vulnerabilities associated with TCP/IP. Firewalls generally implement one of two basic design policies:
permit any service unless it is expressly denied, and
deny any service unless it is expressly permitted.
A firewall that implements the first policy allows all services to pass into the site by default, with the exception of those services that the service access policy has identified as disallowed. A firewall that implements the second policy denies all services by default, but then passes those services that have been identified as allowed. This second policy follows the classic access model used in all areas of information security.

The first policy is less desirable, since it offers more avenues for

getting around the firewall, e.g., users could access new services currently not denied by the policy or run denied services at non-standard TCP/UDP ports that aren't denied by the policy. Certain services such as X Windows, FTP, Archie, and RPC cannot be filtered easily and are better accommodated by a firewall that implements the first policy. The second policy is stronger and safer, but it is more difficult to implement and may impact users more in that certain services such as those just mentioned may have to be blocked or restricted more heavily.

The relationship between the high level service access policy and its lower level counterpart is reflected in the discussion above. This relationship exists because the implementation of the service access policy is so heavily dependent upon the capabilities and limitations of the firewall system, as well as the inherent security problems associated with the wanted Internet services. For example, wanted services defined in the service access policy may have to be denied if the inherent security problems in these services cannot be effectively controlled by the lower level policy and if the security of the network takes precedence over other factors. On the other hand, an organization that is heavily dependent on these services to meet its mission may have to accept higher risk and allow access to these services.

4.15 Limitation of Firewall Limitations

Firewalls are a good first step in protecting your organization from hackers. But they do have their limitations.

Viruses. Not all firewalls offer full protection against computer viruses as there are many ways to encode files and transfer them over the Internet.
Attacks. Firewalls can’t protect against attacks that don’t go through the firewall. For example, your firewall may restrict access from the Internet, but may not protect your equipment from dial in access to

your computer systems.

Architecture. Consistent overall organization security architecture: Firewalls reflect the overall level of security in the network. An architecture that depends upon one method of security or one security mechanism has a single point of failure. A failure in its entirety, or through a software application bug, may open the company to intruders.

Monitoring. Some firewalls can notify you if a perceived threat occurs, however, they can't notify you if someone has hacked into your network. Many organizations find they need additional hardware, software and network monitoring tools.

Encryption. While firewalls and Virtual Private Networks (VPNs) are helpful, they don't encrypt confidential documents and E-mail messages sent within your organization or to outside business contacts. Formalized procedures and tools are needed to provide protection of your confidential documents and electronic communications.

Vulnerabilities. Like a deadbolt lock on a front door, a firewall can't tell you if there are other vulnerabilities that might allow a hacker access to your internal network. Organizations frequently rely on Security Vulnerability Assessments to help them manage their risks.

Check Your Progress-2

1. Pretty good privacy (PGP) is used in
a) browser security b) email security
c) FTP security d) none of the mentioned

2. In ……., the virus places an identical copy of itself into other programs or into certain system areas on the disk.
a) Dormant phase b) Propagation phase
c) Triggering phase d) Execution phase

3. Preventing Virus Infection:
a) Use only commercial software acquired from reliable, well established vendors
b) Test all old software on an isolated computer
c) Make many copies for your software
d) Others

4. Mechanism to protect private networks from outside attack is
a) Firewall b) Antivirus
c) Digital signature d) Formatting

5. Firewalls operate by
a) The pre-purchase phase.
b) isolating Intranet from Extranet.

c) Screening packets to/from the Network and provide controllable filtering of network traffic.
d) None of the above.

6. Gaining unauthorised access to a computer system would fall under which category of computer crime?
a) Hacking.
b) Destruction of data and software.
c) Theft of services.
d) Data theft.

4.16 Let Us Sum Up

1. Web security is a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organizations.

2. The security problems affecting the three areas of Internet commerce :Credit Card Transactions, Virtual Private Networks, Digtal Certification.

3. Ways to protect information from eavesdropping as it travels through a network: Physically secure the network, Hide the information, Encrypt the information so that it cannot be decoded by any party who is not in possession of the proper key.

4.Secure Socket Layer (SSL), a system for automatically encrypting information as it is sent over the Internet and decrypting it before it is used.

5.Privacy is the control over one's personal data and security ,the attempted access to data by unauthorized others.

6. According to corporate E-mail privacy policy ,there should be no expectation of privacy, and any e-mail is subject to review.

7. Denial of Service (DoS) Attacks. Increasingly prevalent Denial of Service (DoS) attacks, aim not to steal information, but to disable a device or network so users no longer have access to network resources.

8. Privacy software is software built to protect the privacy of its users.

9. Pretty Good Privacy, GNU Privacy Guard, Secure Shell, Mozilla Firefox, Portable Edition are ssome of privacy software.

10. Hacker are skilled programmer proficient in machine code and computer operating systems. In particular, these individuals could always hack on an unsatisfactory system to solve problems and engage in a little software company espionage by interpreting a competitor's code.

11. A computer virus is a small software program that spreads from one computer to another and interferes with computer operation.

12. Anti-virus software searches for evidence of the presence of viral programs, worm, bombs, and Trojan horses by checking for the characteristic appearances or behaviors that is typical of these programs.

13. An Internet firewall is a device that is designed to protect your computer from data and viruses that you do not want.

14. The primary components of a firewall are:a) Network policy, b) Advanced authentication mechanisms,c) Packet filtering, and d) Application gateways.

15. two basic design policies of firewall: to permit any service unless

it is expressly denied, and deny any service unless it is expressly permitted.

4.17 Answers to Check Your Progress-1

1. a, 2. a, 3. b, 4. a, 5. c, 6. d

Answers to Check Your Progress-2

1. b, 2. b, 3. a, 4. a, 5.c , 6. a

4.18 Further Readings

1 D. Whitley, E-Commerce-Strategy, Technologies and Applications, TMH.

2 K.K.Bajaj, E-Commerce - The Cutting Edge of Business, TMH.

3 W. Clarke, E-Commerce through ASP, BPB.

4 M.Reynolds, Beginning E-Commerce with VB, ASP, SQL Server 7.0 and MTS, Wrox.

4.19 MODEL QUESTIONS

1. Explain web security. What are the types of security features used in client server types of network?
2. Explain briefly how firewalls protect network.
3. What is a computer virus? How does it spreads ?
3. Explain the use of SSL to secure the network.
4. Discuss any two popular techniques to ensure secured transac-

5.2 INTRODUCTION

When we use the Internet, we're not always just clicking around and passively taking in information, such as reading news articles or blog posts — a great deal of our time online involves sending others our own information. Ordering something over the Internet, whether it's a book, a CD or anything else from an online vendor, or signing up for an online account, requires entering in a good deal of sensitive personal information. A typical transaction might include not only our names,e-mail addresses and physical address and phone number, but also passwords and personal identification numbers (PINs).

The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way we live and work. It's extremely easy to buy and sell goods all over the world while sitting in front of a laptop. But security is a major concern on the Internet, especially when you're using it to send sensitive information between parties.

There's a whole lot of information that we don't want other people to see, such as: Credit-card information, Social Security numbers, Private correspondence, Personal details, Sensitive company information, Bank-account information.

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. But the most popular forms of security all rely on ***encryption***, the process of encoding information in such a way that only the person (or computer) with the key can decode it.

5.3 ENCRYPTION AND DECRYPTION TECHNIQUES

There are two basic techniques for encrypting information: symmetric encryption also called secret key encryption and asymmetric en-

5.4 SYMMETRIC ENCRYPTION- KEYS AND DATA ENCRYPTION STANDARD (DES)

Just like two Spartan generals sending messages to each other, computers using symmetric-key encryption to send information between each other must have the same key. In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.
The same goes for computers, but, of course, the keys are usually much longer. The first major symmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES).

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

be obsolete. Yet, it is often used in conjunction with Triple DES. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary, such as instances where the keys must be increased to 64 bits in length. Known for its compatibility and flexibility, software can easily be converted for Triple DES inclusion.

Triple DES encrypts input data three times. The three keys are referred to as k1, k2 and k3. This technology is contained within the standard of ANSIX9.52. Triple DES is backward compatible with regular DES.

5.6 ASYMMETRIC ENCRYPTION- SECRET KEY ENCRYPTION, PUBLIC AND PRIVATE PAIR KEY ENCRYPTION

Asymmetric encryption or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

An asymmetric algorithm, is a trap door or one-way function. Such a function is easy to perform in one direction, but difficult or impossible to reverse. For example, it is easy to compute the product of two given numbers, but it is computationally much harder to find the two factors given only their product. Given both the product and one of the factors, it is easy to compute the second factor, which demonstrates the fact that the hard direction of the computation can be made easy when access to some secret key is given. The function used, the algorithm, is known universally. This knowledge does not enable the decryption of the message. The only added information that is necessary and sufficient for decryption is the recipient's

encryption.
c) The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
d) The encrypted message contains the function for decryption which identifies the Private Key.

4.Which is the largest disadvantage of the symmetric Encryption?
a) More complex and therefore more time-consuming calculations.
b) Problem of the secure transmission of the Secret Key.
c) Less secure encryption function.
d) Isn't used any more.

5.Which is the principle of the encryption using a key?
a) The key indicates which funcion is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
b) The key contains the secret function for encryption including parameters. Only a password can activate the key.
c) All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
d) The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.

5.7 AUTHORIZATION AND AUTHENTICATION

Authentication verifies who you are. For example, you can login into your Unix server using the ssh client, or access your email server using the POP3 and SMTP client. Usually, PAM (Pluggable Authentication Modules) are used as low-level authentication schemes into a high-level application programming interface (API), which allows programs that rely on authentication to be written independently of the underlying authentication scheme.

access a particular authenticated user called Ram should have. For example, Ram can compile programs using GNU gcc compilers but not allowed to upload or download files. So
Is user Ram authorized to access resource called ABC?
Is user Ram authorized to perform operation XYZ?
Is user Ram authorized to perform operation P on resource R?
Is user Ram authorized to download or upload files?
Is user Ram authorized to apply patches to the Unix systems?
Is user Ram authorized to make backups?
In this example Unix server used the combination of authentication and authorization to secure the system. The system ensures that user claiming to be vivek is the really user Ram and thus prevent unauthorized users from gaining access to secured resources running on the Unix server at www.world.org.

5.8 DIGITAL SIGNATURES

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

A digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds both of them together. Digital signatures ensures the authenticity of the signer. Any changes made to the document after it has been signed invalidate the signature, thereby protecting against signature forgery and information tampering. As such, digital signatures help organizations sustain signer authenticity, accountability, data integrity and the non-repudiation of signed electronic documents and forms.

Working of Digital Signature using an example:
Using Bob and Alice, we can illustrate how a digital signature is ap-

with her calculated one - Alice's software then calculates the document hash of the received document and compares it with the original document hash. If they are the same, the signed document has not been altered.

5.9 VIRTUAL PRIVATE NETWORK

As a business grows, it might expand to multiple shops or offices across the country and around the world. To keep things running efficiently, the people working in those locations need a fast, secure and reliable way to share information across computer networks. In addition, traveling employees like salespeople need an equally secure and reliable way to connect to their business's computer network from remote locations.

One popular technology to accomplish these goals is a VPN (virtual private network). A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses “virtual” connections routed through the Internet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security -- anyone intercepting theencrypted data can't read it.

VPN was not the first technology to make remote connections. Several years ago, the most common way to connect computers between multiple offices was by using a leased line. Leased lines, such as ISDN (integrated services digital network, 128 Kbps), are private network connections that a telecommunications company could lease to its customers. Leased lines provided a company with a way to expand its private network beyond its immediate geographic area. These connections form a single wide-area network (WAN) for the business. Though leased lines are reliable and secure, the leases are expensive, with costs rising as the distance between offices increases.

nect to the VPN with no trouble at any time (unless hours are restricted), and the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.

Scalability -- As a business grows, it should be able to extend its VPN services to handle that growth without replacing the VPN technology altogether.

CHECK YOUR PROGRESS-2

1. Authentication is:

a) Modification

b) Insertion

c) Hard to assure identity of user on a remote system

d) Others

2. A VPN relies on a special protocol understood only by the VPN software to transmit packets, a technique called _____.

a) encryption

b) packet switching

c) tunneling

d) packet hiding

3. A digital signature is

a) scanned signature b) signature in binary form

c) encrypting information d) handwritten signature

4. Message _____ means that the sender and the receiver expect privacy.

a) confidentiality b) integrity

c) authentication d) none of the above

5.A(n) _____ is a pseudo private data network that uses public bandwidth in combination with a tunneling

7. Any connection attempt must be both authenticated and authorized by the system.

8.A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic.

9. A VPN is a private network that uses a public network usually the Internet to connect remote sites or users together.

10. A VPN's purpose is providing a secure and reliable private connection between computer networks over an existing public network, typically the Internet.

5.11 ANSWERS TO CHECK YOUR PROGRESS

Answers to Check Your Progress-1

1. d, 2. b, 3. b, 4. b, 5. c, 6.

Answers to Check Your Progress-2

1.c , 2. a, 3. c, 4. c, 5. c, 6. a

5.12 FURTHER READINGS

1 D. Whitley, E-Commerce-Strategy, Technologies and Applications, TMH.

2 K.K.Bajaj, E-Commerce - The Cutting Edge of Business, TMH.

3 W. Clarke, E-Commerce through ASP, BPB.

4 M.Reynolds, Beginning E-Commerce with VB, ASP, SQL Server 7.0 and MTS, Wrox.

UNIT 6: INTRANET AND EXTRANET

UNIT STRUCTURE

6.1 LEARNING OBJECTIVES

After going through this unit, you will be able to :

- define Intranet
- describe the technological structure of Intranet
- explain the developmental strategy of Intranet
- explain the difference of Intranet with Extranet
- define B2B application
- describe the role of Intranet in B2B application

6.2 INTRODUCTION

From the discussion of first three units we must have got an idea about our surrounding technology, about the modern, upcoming and emerging technology. We also have got the idea of the power and use of these technologies in our society. As our data are in Web, anyone can hack and crack our data. How to make our data secure and about the computer viruses are all discussed details in unit 4 and 5. Till now we were discussed all about Internet which is global, means covering the whole globe. But there may be some companies having individual components, having their own design, algorithm, protocol, but they can work as same as the Internet. These are called Intranet. Intranets are accessible only within the company.

In this unit, we are going to discuss about this Intranet technology and its structure. We also will discuss the advantages and disadvantages of this technology. In this unit we will give the concept of another network called Extranet, an extension of Intranet. Its differences with Intranet are also discussed here. At last of this unit, the concept of B2B application and the role of Intranet on it is giving.

6.3 DEFINITION OF INTRANET

Intranet is same as Internet technology that we discussed in earlier unit, but restricted within an organization. It works same as Internet. It has the same design, same algorithm and has same protocol as Internet. We may say Intranet is a computer network that uses Internet technology to share information within an organization. It is a private analog of the Internet or private extension of Internet that confined to an organization. An Intranet may host multiple private websites. For small

The first Intranet websites and home pages were published in the year 1991.

organizations, intranets are created simply by using private IP address ranges, such as 192.168.0.0/16. In these cases, the intranet can only be directly accessed from a computer in the local network.

In many organizations, intranets are protected from unauthorized external access by means of a network gateway and firewall. It is highly secured and safe. Since it has the firewall, it cannot be accessed by the external people.

The first Intranet website appeared in non-educational organizations in the year 1994.

Intranets are basically managed by the communicators, HR and CIO departments of large organization.

6.3.1 Uses of Intranet

Intranets and their use are growing rapidly. The applications of Intranet can be classified as:

- **Communication and collaboration:** Intranet offers the companies to share information very quickly and reliably. Intranets are the platform for corporate culture-change. For example, a large numbers of employees can discuss their key issues in an intranet forum application where ever they are in world. It plays a significant role in the calendaring of the activities of employees.

- **Web publishing and Intranet management:** Intranets are used typically to publish web pages about company events, health and safety policies, and staff newsletters. It helps in eliminating paperwork and speed up workflows. Another example would be a hospital providing local GPs with access to a booking system so they can make appointments for their patients.

- **Business operation and management:** Intranet helps the organizations to access the important data to do their operations. The corporate data is also accessed through these kinds of networks. In business private messages can send through public network, called intranet services, using special encryption /decryption and other security safeguards.

User can access public internet through firewall servers within their Intranet services. In large intranets, website traffic is often similar to public website traffic and can be better understood by using web metrics software to track overall activity.

6.3.2 Characteristics of Intranet

The characteristics of Intranet are same as Internet. It is built in the same concepts and same technologies like Internet. Intranet has the **Client-Server Computing** and the **Intranet Protocol Suite (TCP/IP)**. An intranet can be understood as a private analogy of the Internet, or as a private extension of the Internet confined to an organization. The well known Internet protocols such as HTTP (web services), SMTP (e-mail), and FTP (file transfer protocol) are also found in an intranet.

6.3.3 Intranet Software

As we know that to create any application, there should be some software. Like to build any Intranet, we need to take help of software. The well known software used for creating Intranet is the *Microsoft SharePoint*. Though there is some other software also available in the market to build Intranet, it is found that around 50% of all Intranets are developed using SharePoint. Other popular intranet software includes:

- Autonomy Corporation

- Atlassian Confluence
- Drupal
- eXo Platform
- Google Sites
- IBM Websphere
- Intranet Dashboard
- Jive Software
- Joomla
- Liferay
- Lotus Notes
- OpenText
- Plone (software)
- SAP NetWeaver Portal
- Sitecore
- Oracle Fusion Middleware

6.3.4 Advantages and Disadvantage of Intranet

The advantages of using Intranet are:

- **Workforce productivity**: Intranets helps users to locate and view relevant information faster. With the help of a web browser interface, users can access their required data held in any databases and can make their own database available at anytime for others. It increases employees' ability to perform their jobs faster, more accurately, and with confidence that they have the right information. It also helps to improve the services provided to the users.

- **Decrease Searching Time**: Intranets allow organizations to distribute information to employees on an *as-needed* basis. Employees may link to relevant information at their convenience, rather than being distracted indiscriminately by email.

- **Improve Communications**: Intranets can serve as powerful tools for communication within an organization. The type of information that can easily be conveyed is the purpose of the initiative and what the initiative is aiming to achieve, who is driving the initiative, results achieved to date, and who to speak to for more information. By providing this information on the intranet, staff has the opportunity to keep up-to-date with the strategic focus of the organization.

- **Web publishing:** Intranet web publishing allows cumbersome corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. For example, employee manuals, benefits documents, company policies, business standards, news feeds, and even training, can be accessed using common Internet standards. Because each business unit can update the a document, the most recent version is usually available to employees using the intranet.

- **Business operations and management**: Intranets are platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.

- **Cost-effective**: Users can view information and data via web-browser rather than maintaining internal physical documents. This can potentially save the business money on printing and duplicating documents. It also decreases the document maintenance overhead.

- **Enhance collaboration**: Information is easily accessible by all authorized users, which enables teamwork.

- **Platform independent**: Standards-compliant web browsers are available for Windows, Mac, and UNIX.

- **Promote common corporate culture**: Every user has the ability to view the same information within the Intranet.

- **Immediate updates**: Intranets make it possible to provide their audience with "live" changes so they are kept up-to-date, which can limit a company's liability.

- **Supports a distributed computing architecture**: The intranet can also be linked to a company's management information system, for example a time keeping system.

Though Intranet has many advantages, it has few disadvantages also. They are:

• **Security issues**: In implementing networks in organization, anyone can access that and therefore can use the password and ID illegally.

• **Dependence on computer**: Peoples are more dependent in computer now-a-days, which may affect negatively on the performance of the employees. They may not take work seriously as before

• **Time**: Time is needed for the training of the employees to use new tools of network.

CHECK YOUR PROGRESS 1

1. Fill in the blanks

a) The first Intranet websites and home pages were published in the year _____.

b) Standards-compliant web browsers are available for Windows, Mac, and UNIX is called _____.

c) An _____ is a private analogy of the Internet.

d) The well known software used for creating Intranet is the _____.

e) For large organizations, Intranets are basically managed by the _____, _____ or _____.

2. Write True or False

a) An Intranet is a private extension of the Internet

b) Intranet Improves Communications.

c) Intranet protocol does not use HTTP.

d) Intranet is very costly in respect of implementation and maintenance.

e) The first Intranet website appeared in non-educational organizations in the year 1994.

6.4 COMPONENS OF INTRANET TECHNOLOGY STRUCTURE

Intranet technology structure is the content structure of an Intranet or a framework of how content is categorized and labeled in relation to other content. In short, we can say that it is the art or science of structuring, labeling and categorizing content of an organization. It is the organizational chart having various parent and sub-categories and describes how they related to each other. A sample Intranet structure of an organization is given below:

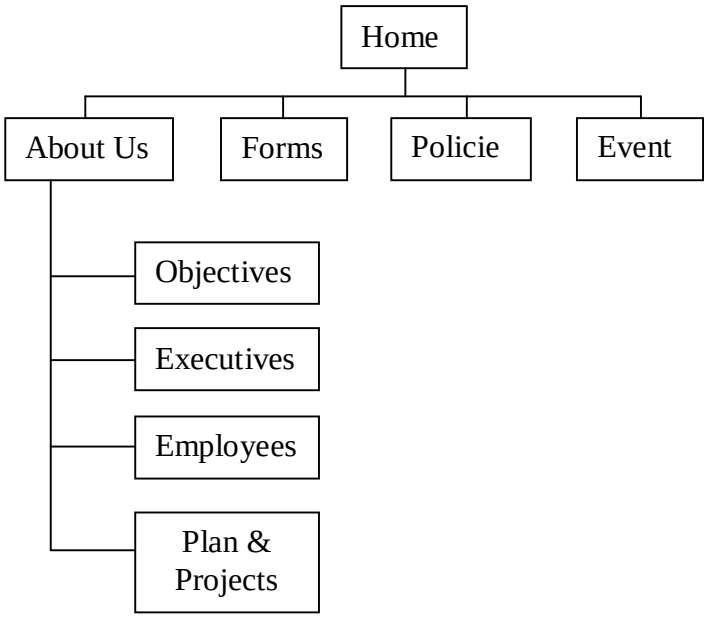

Figure 6.1: Sample Intranet structure

In this way for each parent structure, there may be some sub-structure and the whole structure may vary organizational needs and requirements. In the Intranet structure few components are found to be very common mainly at homepages and frequently used pages. They are:

Description: The first component in general Intranet site is the description section. This section contains the messages from originator, founder or owner of the organization for which the Intranet site has been built. This is the best portion to share messages to others by the leader of the company. It provides company news, inspiring comments and key issues of the companies to make awareness about the company.

Image sample: There may be an image portion of the leader of the company with the massages of the homepage. Intranet site uses this portion to make the site attractive and impressive.

Update frequency: The update frequency varies company wise. Some may update on a daily basis, some may weekly, bi-weekly, monthly basis and so on. But it is

recommended that this frequency should not be more than quarterly basis. The less frequency of update again indicates the low priority Intranet or not a critical business application of the organization.

Value proposition: This is basically the leadership blog or leadership news components. It displays in the homepage if there is not enough dynamic contents. This component can be valuable if updates on a frequent basis.

Related Link: In many intranets, links were immensely helpful, particularly when they were designed consistently.

6.5 DEVELOPMENT OF INTRANET

Developing a usable and consistent Intranet is a challenging task though the process of creating an effective intranet is much in common with creation of an external website. We simply need a user-friendly interface, architecture to navigate, accurate content with an appropriate voice and visual elements. But we should have to follow few steps from thinking of a site to appropriately launch it. The development includes the following phases:

Phase 1: Problem Definition and Requirement Analysis

This phase is the analysis phase. Before developing an Intranet for an organization, there are some issues to be followed by the organization. The issues are:

a) **Selection of team**: First of all, there should be a planning about what contents to be included and what not, and also about what technology has to be used. Generally a person or a team of persons is employed by the organization to determine about the contents of the site.

b) **Cost benefit analysis**: After selecting the team, they have to assemble for discussion on cost, size and the functionality of the site. They have to decide about:

- Who will be the intranet's primary audience? All employees? Or only certain departments?
- What are the intranet's goals?
- How will the success of the Intranet be measured?
- What types of documents and which corporate databases will need to be accessed?
- What Web-based applications will be accessible from the intranet?
- How will the site be structured? What will be on the homepage, the different main landing pages and sub-pages?
- Will everyone be allowed to publish content to the intranet or only certain employees?
- Who will be in charge of communicating editorial guidelines and maintaining editorial consistency?

c) **Technical maintenance:** After deciding everything, the team has to decide about the technical maintenance that includes:

- Who will be in charge of configuring and maintaining the Web server, in-house information technology staff or by contractors?
- What security precautions need to be in place like firewalls or other security software?
- How much network bandwidth will be required according to the used audio, video and graphics?

- What content management system (CMS) will be used to create and publish content and how the employees be trained for that?
- Who will be the contact for technical issues/questions about the CMS?
- How will the company back up intranet data? How does intranet data fit into the company's larger disaster recovery plan

d) **Preparing proposal:** The team has to prepare a proposal for the budget and has to present to the head of the organization. This budget includes the following items:

- Web servers
- People to administer servers (in-house or contractors)
- Web development and design (in-house or contractors)
- Content management system
- Application development (software and personnel)
- Security hardware and software
- Long-term maintenance costs

Once the budget is approved, it is ready to set up and develop the site.

Phase 2: Design the Intranet

After finish analyzing the Intranet site, the next job is to design the site. According to the decision taken in the first phase, the team has to deliver all their needs to the designer. The design part includes the structural and technical design of the site. At times, this phase runs

concurrently with both the Discover and Implementation stages. At the end of this phase, all of the tools needed for information access, security, site monitoring, content management and issue tracking will have been designed.

There are many design methodologies. The most common methodologies are *Rapid Prototyping* and *Structured Development*. Rapid prototyping is basically used for small to medium projects and structured development is used for large and complex projects.

Phase 3: Implement the Intranet

Once the requirement analysis is well underway, the focus team is becoming happy with the design part, it is now the time to begin implementing the site. This phase guides the development team through the implementation of the systems designed in the last stage. This phase includes:

- coordinating hardware and software
- network and hardware installation
- software development
- preparing documentation guide and manual
- preparing reviews and
- testing

At times, this phase runs concurrently with both the Discover and Design stages. At the end of this phase, all systems should be in place and the site should be ready for launch.

Phase 4: Test and Review

Testing and Reviews take place throughout the development cycle, including prototyping, development, deployment, operations, and enhancements. It never ends. It

is wise to place a single individual in charge of testing and reviews. This is not a popular job, but it is critical for developing a system that works and meets each of the requirements. There should be an appropriate person to give authority to look after these. Usually a quality assurance engineer is engaged for that. Testing is time consuming, tedious work and preparing for reviews and analyzing results can take much longer time.

Phase 5: Launch the Intranet

This phase guides the development team through many of the follow through activities that can make a huge impact on the success of the site. These activities include:

- Site promotion
- Gathering feedback
- Software distribution
- Post mortem

CHECK YOUR PROGRESS 2

3. Fill in the blanks

a) _____ methodology is basically used for small to medium projects.

b) The common Intranet design methodology used for large and complex projects is _____.

c) The first component in general Intranet site is the _____.

d) Intranet site uses _____ portion to make the site attractive and impressive.

e) _____ is basically the leadership blog or leadership news components.

4. Write True or False

a) Rapid prototyping is a common extranet design methodology.

b) Structured development is the methodology basically used for small to medium projects.

c) Intranet technology structure is nothing but an organizational chart.
d) Testing and Reviews take place throughout the development cycle
e) The design part of Intranet includes the structural and technical design of the site.

6.6 EXTRANET: DEFINITION

Till this we have discussed only about Intranet. But there is another term related to Intranet which is called Extranet. It is also a kind of network where external people may also be able to access the site. It is a private network that uses the public telecommunication system to securely share information. The applications of extranet are same as Intranet that we have discussed before.

An Extranet should be more efficient because everyone can access the same data in the same format. Because all communications can be encrypted over a VPN (Virtual Private Network), it should also be more secure than sending data over the public internet. We can say that extranet is a business to business communication that uses Internet technology. So,

Extranet = Business to Business Commerce using Internet technology.

The successor of Electronic Data Interchange (EDI) which was and in some cases still is based on extranet or leased communication lines.

6.6.1 Business Value of Extranets

We pointed out that extranet is use in business to business. It increases the business value as:

- Extranet technology makes it easier and faster for customers and suppliers to access resources.

- Extranets enable a company to offer new kinds of interactive Web-enabled services to their business partners.

- Extranets are a way that a business can build and strengthen strategic relationships with its customers and suppliers.

- Extranets can enable and improve collaboration by a business with its customers and other business partners.

- Extranets facilitate an online, interactive product development, marketing, and customer-focused process that can bring better designed products to market faster.

6.6.2 Difference Between Extranet and Intranet

The main differences are that in Intranet, the applications are only accessible to the authorize members of the organization through unique ID and passwords. But Extranet, where external bodies are also made part and they can also access the site. It reduces cost of the business as vendors, suppliers, partners, customers and all other businesses can see a site of an organization. Since extranet shares organizational information, it increases the efficiency. Extranet is used when an organization do the business to business transactions. It is basically the link of intranets. The secure protocols will be used to connect the intranets. Extranet replaces traditional Electronic Data Interchange systems and networks in many cases.

What we have seen from our discussion that Intranets and extranets both work and feel like the Internet.

They enable and improve collaboration within a business, and with customers and other business partners. In many respects, intranets, extranets and enterprise collaboration help a business gain and sustain a competitive advantage.

6.7 ROLE OF INTRANET IN B2B APPLICATION

B2B or Business-to-business commerce is a fundamental transformation of trade. We heard the name e-businesses or electronic data interchange (EDI). The forefather of B2B is the EDI. But EDI was very costly to implement and maintain. It had required skilled trainer and technician. Development of Intranet has overcome this. It reduces the cost. Now B2B is available to companies of all sizes. The primary roles of a B2B web site are aggregating multiple extranets into a single Web site and providing the security context in which companies can safely conduct business online with other companies and individuals. Developers of Intranet are mainly responsible for the security of the B2B applications.

Intranet has a major role in B2B applications. Because of Intranet, e-businesses have the following advantages:

- An easily accessed customer interface. Intranet makes it possible for customers to access video lectures, presentations from their desktop.
- A way to distribute information, real-time access to information.
- A worldwide pipe-line.
- Intranet integrates all unequal applications installed in different environments to consolidate information like:
    - Enterprise Resource Planning (ERP)
    - Customer Relationship Management (CRM)
    - Sales Force Automation (SFA)

Intranet gives most interactive and extensible business communication solutions to its valued clients. It gives great boost to the international businesses and enhances precision and effectiveness of the team work that has been driving the companies to the ever new horizons of success and exposure. Intranet provides more security, accuracy and speed which is very much necessary in B2B applications in order to keep the business relations intact. The following services are possible in B2B applications because of Intranet communication system:

Call centre services: Provides inbound and outbound customer relationship management solutions.

Outsourcing: Customers can have the facility of hiring services for typing, data entry, virtual assistance and many more.

CHECK YOUR PROGRESS 3

5. Fill in the blanks

a. Applications of Intranet are only accessible to the _____ of the organization.
b. In _____ customers are able to access all information stored in the site of the organization.
c. Call centre services are possible in _____.
d. _____ is the forefather of B2B applications.
e. _____ is a B2B communication that uses Internet technology.

6. Write True or False

a) External bodies are also made part and they can also access the site in Intranet.

b) Extranet technology makes it easier and faster for customers and suppliers to access resources.
c) Intranet integrates all unequal applications installed in different environments.
d) Outsourcing is possible because of Intranet and Extranet.
e) Developers of Intranet are not responsible for security of B2B applications.

6.8 LET US SUM UP

From this unit we have got the idea about Intranet, Extranet and B2B applications. We came to know that Intranet works same as Internet. Its protocol and algorithm is also same as Internet. But Intranet is not open for all, it is limited to an organization and the people who have access permission, they can only access it. This is the main difference between Internet and Extranet. An Intranet may host many multiple private websites. Sometimes some Intranets uses private IP addresses and such Intranets are accessible from a computer of local network.

Intranet has varieties of applications and applications are growing very fast. *Communication and collaboration, Web publishing and Intranet management, Business operation and management* are three main applications of Intranet we discussed in this chapter. User can access public internet through firewall servers within their Intranet services.

We came to know that *Microsoft SharePoint* is the well known software to develop Intranet website. Around 50% Intranets are developed with this software. The other available Intranet developing software are listed before.

There are lots of advantages of using Intranet which has discussed thoroughly in section 6.3.4. We also had discussed few disadvantages in this section.

Section 6.4 is the details of the structure of an Intranet site. Section 6.5 gives the idea of developing an Intranet site from beginning to launching. What restrictions and what types of steps have to follow to create an attractive and user friendly Intranet site is also discussed here in this section.

In this chapter we also discussed another kind of network related to Intranet is called Extranet. In extranet, external people also may able to access the site. The applications, technology and protocol that uses by Extranet is same Intranet. The only difference is that extranet is more efficient because external people also can access extranet which is not possible for Intranet. Extranet is a business to business communication that uses Internet technology.

The result of Intranet and Extranet is the business-focused e-commerce. E-commerce is through business-to-consumer (B2C), business-to-business (B2B), business-to-employee (B2E) and consumer-to-consumer (C2C). Section 6.7 discusses the role of intranet in B2B application. B2B is now available to companies of all sizes.

6.9 ANSWERS TO CHECK YOUR PROGRESS

1. a) 1991 b) platform independent
   c) intranet d) Microsoft SharePoint
   e) communicators, HR, CIO departments
2. a) T b) T c) F d) F e) T
3. a) Rapid prototyping b) structured development
   c) description section d) image sample
   e) Value proposition
4. a) F b)F c) T d) T e) T

5. a) authorize members b) Extranet
   c) B2B applications d) EDI e) Extranet
6. a) F b) T c) T d) T e) F

6.10 FURTHER READINGS

1. Tanenbaum A.S. C*omputer Network*, Prentice Hall, India.
2. Robinson (2001). *Implementing security in B2B applications*.
3. Ward T. (2008). *Intranet Information Architecture*
4. Schaffer E. M. (2003). *How to develop a corporate Intranet standard*.

6.11 MODEL QUESTIONS

1. What do you mean by Intranet? How it is different from Internet technology?
2. What are the advantages of using Intranet over Internet?
3. Explain the use and characteristics of Intranet.
4. What software is mostly used by developers to build an Intranet site? List any five available software that is use to build an Intranet site.
5. Explain Intranet organizational chart with a suitable example.
6. Explain the phases of to develop an Intranet.
7. What do you mean by Extranet? How it is different from Intranet technology?
8. What is EDI and how it is related to B2B application?
9. What is the role of Intranet in B2B application?
10. Why are companies installing Intranets?
11. What are major issues that you need to consider when building a intranet?

*****

UNIT 7: ELECTRONIC PAYMENT SYSTEM

UNIT STRUCTURE

7.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- learn the Electronic payment systems and the way it affects business
- learn about the protocol used to transact over different networks
- describe different electronic payment instruments
- learn about online banking and the electronic data interchange

7.2 INTRODUCTION

Electronic communication has changed the way the companies conduct business with one another. With the development in technology, the selling and purchasing of goods over the Internet has become easier and this has helped the growth of E-commerce over the time. Electronic payment systems have become more popular with the increased use of Internet shopping. It is a part of electronic commerce transactions. E-payment services are a convenient and efficient way to do financial transaction. People generally think of E payment as referring to the online transactions over the Internet.

7.3 OVERVIEW OF ELECTRONIC PAYMENT

A payment system is a way to transfer exchange of value between buyers and sellers in a transaction. It facilitates the exchange of goods and services in an economy.

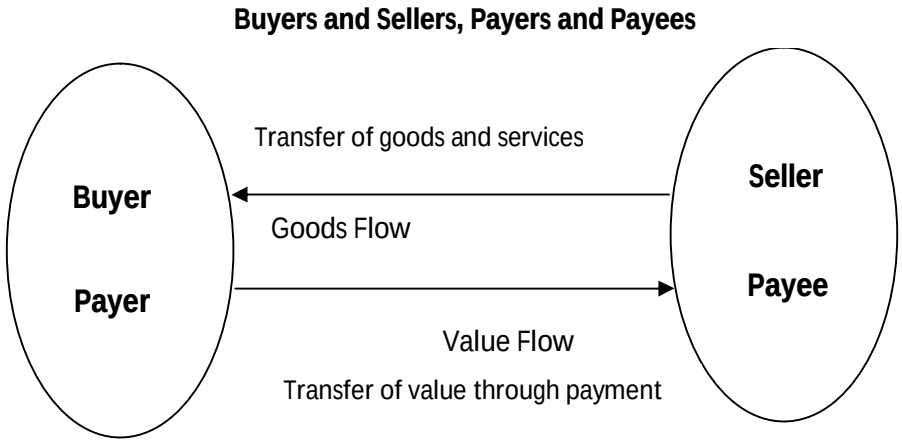

Figure 7.1

A payment system consists of a various set of “payment instruments” like cash, checks, debit and credit cards and e-money. These instruments can be

used to purchase goods and services, to transfer funds from one person to another and also to make financial investments.

The Electronic Payment System (EPS) involves a customer (payer) who makes a payment and a seller or merchant (payee) who receives the payment. In E-payments, money is transferred from the payer to the payee. This process involves a financial institution like a bank. It allows a customer to purchase things and pay online. E-commerce has changed the world of business. The electronic payment systems has increased the efficiency and improved the security thereby making these systems more convenient for the customers.

Electronic payment refers to paperless monetary transaction. It has reduced the paper works, transaction costs and labour costs. Being user friendly and less time consuming, it has helped the businesses worldwide to expand their market.

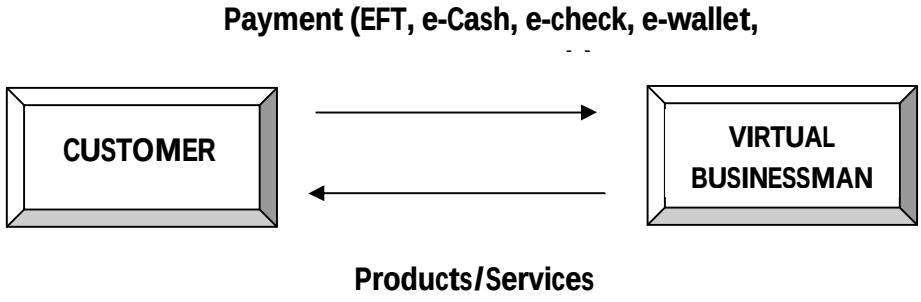

Figure 7.2: ElectronicPayment Scheme

The advantage of E-payment systems are

- Speed and convenience with which the customers can purchase and pay for the products online. Immediate transfer of funds benefits the businesses in several ways. Payments can be made swiftly and remotely using various devices.
- Increase payment efficiency. It reduces the transaction costs.
- Apart from e-commerce, it can also be used other purposes like paying bills, paying taxes etc.

There are two major factors for the development of the Electronic Payment system: reduced operational and payment processing costs and rapid growth of online commerce.

7.4 THE SET PROTOCOL

Secure Electronic Transaction (SET) is a standard protocol that is used for securing credit card transactions over insecure networks. With an increase in E-commerce over internet, there has been a growing security concern regarding the financial transaction between the different parties in a transaction. Most of the payments are made using the credit card and the customers feel insecure to reveal their card information over the Internet as there is a subsequent increase in the credit card frauds registered on the Internet.

Secure payment systems are important to the success of E-commerce. The two leading credit card brands, Visa and MasterCard, developed this common standard to process the card transactionson the Internet which is called as the Secure Electronic Transaction (SET). This standard ensures that the E-payment information travels safely and securely between the two different parties that are involved in the transaction.

Some of the features of SET are as follows:

1. It provides the confidentiality of the payment information
2. It ensures the integrity of the transmitted data
3. It provides cardholder account authentication
4. It also provides merchant authentication
5. Ensures best security and system design techniques to protect the involved parties in an E commerce transaction.

There are four main entities in a SET. They are listed below.

i. Cardholder (Customer)
ii. Merchant (Web Server)
iii. Merchant's Bank (Acquirer)
iv. Issuer (cardholder's bank).

How SET works

The cardholder and the merchant registration need to be done before they can purchase or sell anything on the Internet. This is done by simply filling a registration form by which they are actually authenticating themselves. In the registration process, the applicants do not need to have any digital proof for his identity. Once the registration process is over, the cardholder and the merchant can start transactions, which generally involves the following steps in this protocol.

1. The cardholder (Customer) surfs the websites and selects the product that he will purchase.
2. The customer then sends the order along with the payment information. The purchase order is for the merchant, and the payment information (that is, card information) is forwarded to the merchant's bank.
3. Then the merchant's bank checks with the issuer for payment authorization.
4. The issuer sends the payment authorization to the merchant's bank.
5. Merchant's bank sends authorization to the merchant.
6. The order is then completed by the merchant and a confirmation is sent to the customer.
7. Issuer prints the invoice or the credit card bill to the customer.

The SET protocol relies on cryptography and digital certificate to ensure confidentiality and security. The message is encrypted using a randomly generated key that is further encrypted using the recipient's public key. This is called "digital envelope" and this is sent to the recipient along with the encrypted message.
The recipient decrypts the digital envelope using a private key and then uses the symmetric key to decrypt the original message.

7.5 PAYMENT GATEWAY

The service that automates and authenticates electronic payments made by the customers to the e-commerce merchants is called Payment Gateway. It

acts as the interface between the banks of the customer and the merchant. It allows money transfer between the bank account of the customer and the merchant. The payment gateway is a software application that has algorithms to detect fraud. They can process multiple payment mechanisms including debit cards and smart cards.

Based on the location of the transaction processing code, there are two different types of payment gateways.

1. Secure order form: In this typethe customers are redirected to the website of the payment gateway provider. Once the payment is processed, the customer is returned to the website of that merchant.

2. Merchant side API (application programming interface):In this type,the transaction processing code is on the merchant's web server. The payment gateway is accessed by using API.

CHECK YOUR PROGRESS 1

1. **Fill in the blanks**:

a. _____ facilitates the exchange of goods and services in an economy.

b. Electronic Payment System involves a _____ who makes a payment and a _____ who receives the payment.

c. Electronic payment refers to _____ monetary transaction.

d. _____ is a standard protocol that is used for securing credit card transactions over insecure networks.

e. The SET protocol was developed by _____ and _____.

f. The SET protocol relies on _____ and digital certificate to ensure confidentiality and security.

g. _____ acts as the interface between the banks of the customer and the merchant.

h. Two different types of payment gateways are _____ and _____.

i. The payment gateway is a software application that has algorithms to detect _____.

j. Full form of API is _____.

7.6 PAYMENT TYPES

There are various modes of E-payments. These are:

Digital Tokens

The digital tokens are electronic tokens that are generated by the banks to be used by the customers in e commerce. These are equivalent to the cash given by the banks in physical form. This is a new form of electronic payment system based on electronic tokens. The types of Electronic Tokens used are Cash or Real time, Debit or Prepaid and Credit or Postpaid.

In Cash or Real time, the transactions take place with the help of electronic cash or E-cash. In Debit or Prepaid systems, the users pay in advance for the privilege of getting the information. Examples are Smart cards and electronic purses. In credit or postpaid type of electronic token, the server authenticates and verifies the identity of the customer through the bank. After these processing the transactions take place. Examples of postpaid systems are Credit/Debit cards and electronic checks.

Smart Card

Smart cards are small, portable pocket-sized plastic cards that contain an embedded computer chip used to store relatively large amount of information and can also transact data. They are one of the latest additions to the field of information technology. They come in various sizes ranging from as small as mobile phone prepaid cards to as big as credit/debit cards. The card data is transacted using a card reader. Smart cards can make personal and business data available to the appropriate users.

Smart cards are classified as microprocessor cards and memory cards based on their application. Memory cards are used to simply store the data with

optional security. Microprocessor cards, on the other hand, can add, delete and manipulate information in its card memory.

Apart from storing information, customers can also securely store money in the smart cards which is reduces as per usage. Smart cards have increased the trust by improving the convenience and security of the transactions. They provide for tamper-proof storage of user and account identity. Smart cards also provide important components of security for data exchange via any type network. They can protect data against a varied range of security threats from careless storage of user passwords to system hacks. The transaction costs are reduced by using a smart card. Transactions that require time and paper works can be managed electronically by the customer with a smart card.
Smart cards have two different types of interfaces depending on the way they are used.

1. Contact: This type of smart cards must be inserted into smart card reader making physical contact with the reader. A contact smart card contains a microprocessor chip that makes contact with electrical connectors to transfer data.
2. Contactless: A contactless smart card also contains a microprocessor chip and an antenna embedded inside the card that allows transmission of data to a special card reader without any physical contact. These use radio frequency identification (RFID) technology.

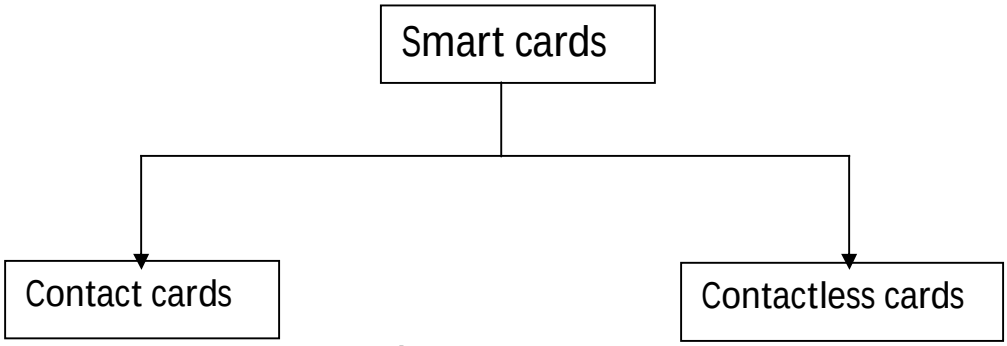

Figure 7.3

A smart card can be programmed for different applications. Applications of Smart card include business, banking/payment, government, healthcare and many others. Smart cards make the information available to those who need it and at the same time it protects the individual privacy by keeping their informational assets safe from hacking and unwanted intrusions. A smart card

can be password protected to guarantee that its only used by the owner. Smart cards can be accessed only using a PIN of the customer. Data is safe as it is stored in an encrypted form.

Smart cards have become a perfect solution for e-commerce transactions.

Credit Card

Credit card is one of the most common forms of electronic payment for the purchase of goods and services globally. It is a small plastic card with a unique number magnetic strip embedded in it. This magnetic strip is used to read the card with the help of a card reader.

When a customer purchases a product with a credit card, the credit card issuer bank pays on behalf of the customer. The customer has a certain time period after which he has to give that amount to the bank. Generally it is a monthly payment cycle. In a credit card system, the entities are-

- Card holder – The customer
- Merchant – The seller who can accept credit card payment
- Card Issuer Bank – The card holder's bank
- Acquirer Bank – The merchant's bank
- Card Brand – Example, Visa or Mastercard

A sample credit is shown below.

Figure 7.4

The credit card payment process is given below:

1. On customer's request, the bank issues and activates a credit card.
2. The merchant validates the customer's identity by asking for approval from the card brand company.
3. The company then authenticates the credit card and the money is paid by credit. The merchant keeps the sales slip.

4. The sales slip is submitted by the merchant to the acquirer bank and gets the service charges paid to him.
5. Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
6. Lastly, the card brand company asks the issuer bank to clear the amount and the amount gets transferred to the card brand company.

The features of a credit card are listed below:

1. Alternative to cash
2. Credit limit. This is of two types – Normal credit limit and Revolving credit limit. Normal credit limit is the credit given by the issuing bank. Revolving credit limit varies with the financial exposure of the credit card holder.
3. Grace period or grace days. It is the minimum number of additional days within which the card holder has to pay his credit card bill without incurring any interest or financial charges.
4. Regular charges. These are of two types – annual charges and additional charges. Annual charges are charges on a yearly basis and the additional charges are collected for other supplementary charges like issuing a new card or an add-on-card etc
5. Helps payment in domestic and foreign currency as it reduces the process of currency conversion
6. Higher fees on cash withdrawals. Generally cash withdrawal fees are quite higher than the regular fees charged for other credit transactions.
7. Additional charges for delay in payment
8. Record keeping of all transactions
9. Service tax
10. Bonus points. To collect many bonus points, the card holder has to carry out a considerable number of transactions through his credit card.
11. Gifts and other offers. The accumulated bonus points at a later stage are redeemed either by converting them into gifts, cash back offers or any other compelling offers.

Credit card standards

There are two standards to securely use credit cards on the web. They are Secure Socket Layer (SSL) encryption and the Secured Electronic Transaction (SET). The SET has already been discussed in section 7.4 above.

The SSL encryption was developed by Netscape in 1994. It is used for secure transmission of vital data between the web browser at the customer's end and the web server at the merchant's end. The SSL uses two types of keys to encrypt private data while transmitting a public key which is known to everyone and is used to encrypt the data, and a private key which is known only to the receiver of the message and is used to decrypt it.

Magnetic strip card

A magnetic strip card is a plastic card that has a magnetic stripe on it. Magnetic stripe is also called a magstripe. The stripe is made up of tiny magnetic particles, like iron, in a plastic film. Each particle is a very tiny bar magnet. The strip at the back of the credit card is a magnetic strip. Credit cards, debit cards have a magnetic strip on the back of the card.

Figure7.5 : Magnetic strip on the back of a card

The magnet bars can be magnetized. The strip looks similar to a piece of cassette tape fastened to the back of a card. Information can be stored in the strip by changing the magnetism of the particles. The card with the strip needs to be “swiped” through a reader or insert in a reader.

These type of cards are widely used for

- Banking (debit or credit cards)
- Tickets issued for transportation
- Key sin some hotels and other buildings
- Systems to track working hours in companies

E-checks

The electronic version of a paper check is the E-check. It is specially designed to meet the electronic transactions of businesses and customers using state-of-the-art security techniques. It is based on the same legal framework and business protocols associated with the traditional paper check and contain the same information as the paper check. The E-check can be directly exchanged between the parties. The amount and necessary bank information from the check is captured and sent through the Automated Clearing House (ACH), which transfers the money to the merchant’s bank account.

The working of E-check is same as that of a paper check. It is just a new high security and high speed payment instrument for providing a convenient and efficient system for on-line transactions. It can be used by small and also large organizations.

Electronic check payment systems offer advantages to both the merchant and the customer with improving efficiency, accuracy and flexibility. Efficiency is improved as it reduces the amount of paper works and the number of people required to handle those works. This in turn reduces the amount of human error in the process which leads to increased accuracy. These type of systems also enables the customers to pay by check 24 hours a day and 7 days a week and receive instant acknowledgement of their payments. Unlike

credit cards, the electronic checks offers more privacy and prevents the merchants from using their information for any other purpose.

The transaction payment sequence in E-check system is shown in the figure below.

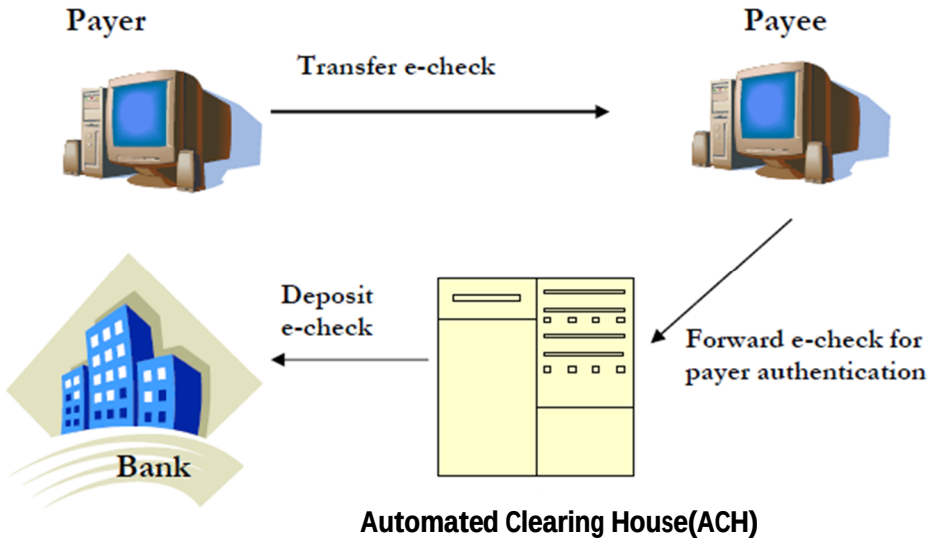

Figure 7.6 Payment sequence in e-Check system

The advantages of E-check are listed below:

a. Fast check processing
b. Low transaction cost
c. Secure and quick settlement of financial obligations.

E-checks are designed to use the security measures like

- Digital signatures
- Authentication
- Digital certificates
- Cryptography
- Encryption
- Duplicate detection

The e-checks leverage and strengthen the relationship of the bank with the account holder.

Credit/Debit card based EPS

The credit/debit card approach in the EPS (Electronic Payment System) means that the money is represented in records in the bank accounts and this information is electronically transferred between the parties over the computer network. When a bank issues a credit/debit card, a personal identification number (PIN) is supplied to the card holder. This PIN needs to be supplied when making monetary transactions using the card.

Debit card, like the credit cards, is a small plastic card with a unique number that is mapped with the bank account number. Banks issues the debit cards to the customer. Whenever a customer makes a payment through the debit card, the amount gets deducted from the debit card holder's bank account immediately. Also to make a payment there must be sufficient balance in the customer's bank account. This is the difference between the debit and credit card, because in case of a credit card the customer may not have sufficient balance in the account.

A sample SBI debit cum ATM card is shown below.

Figure 7.7

Debit card payment is an instant payment system from the customer's account.

CHECK YOUR PROGRESS 2

2. Check True or False

a. Digital tokens can be generated by the merchant company to deal in e-commerce.
b. Smart card is an example of a debit or prepaid card.
c. Contactless smart cards uses radio frequency identification (RFID) technology.
d. When a customer purchases a product with a debit card, the card issuer bank pays on behalf of the customer.
e. Normal credit limit varies with the financial exposure of the credit card holder.
f. There are two credit card standards to securely use them on the web. They are secure socket layer (SSL) encryption and the Secured Electronic Transaction (SET).
g. Credit cards, debit cards have a magnetic strip on the back of the card.
h. E-check increases the amount of human error which leads to decreased accuracy.
i. When a bank issues a credit/debit card, a personal identification number (PIN) is supplied to the card holder.
j. Debit card payment is possible if there is sufficient balance in the customer's bank account.

7.7 TRADITIONAL PAYMENT

Traditional payment methods are called macro payment methods. In a traditional system of buying, the customer can see the product, examine it and then pay for it either by cash, or check or credit card.

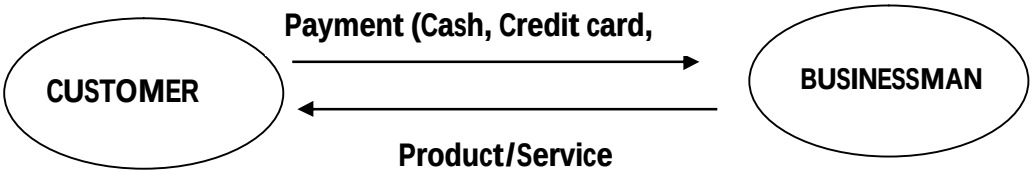

Figure 7.8: Traditional Payment Scheme

In the world of e-commerce, the customer in most cases does not see the actual product and the payment are made electronically. Traditional payment systems are negotiable instruments such as drafts, bank notes, checks, and credit/debit cards. Cash has always been the dominant system of transaction. There are several shortcomings of the traditional payment system for online payments.

- Security risks are involved when exchanging debit and credit cards information over the telephone or Internet. The traditional payment systems for the Internet are easy to steal money and personal information.
- Credit or debit cards do not support individual-to-individual payment transaction.
- Some potential customers with money and intention to pay may not have access to credit cards.
- Lack of efficiency. Some small payments over the Internet using the traditional payment system may cause more overheads in the processing of the payments and transaction. For example, credit cards are not suitable for making small payments as the charges for processing such transactions could even surplus the value of the goods sold.

7.8 ELECTRONIC FUNDS TRANSFER

Electronic fund transfer (EFT) is one of the oldest electronic payment systems. It is an electronic method of making a payment from one bank account to another bank account. The accounts may be in the same bank or in different banks. Money can be transferred using ATM (automated teller machine) with the help of debit/ credit cards or using computer. Internet banking has gained popularity now-a-days. The customer has to login into the bank's website to transfer fund from one account to another. If the fund transfer is between accounts that are in the same bank, the bank transfers the amount. Otherwise if the accounts are in different banks, then the transfer

request is forwarded to ACH (Automated Clearing House) to transfer the fund and the amount is deducted from the customer's account. When the EFT is processed, the customer is notified of the transfer.

EFT is considered to be a safe, reliable and convenient way of conducting business. The advantages of EFT are:

- Improved efficiency
- Simplified accounting
- Improved security
- Reduced cost

EFT uses computer and electronic technology in place of paper transactions. Some common EFT services are -----

1. Automated Teller Machines (ATM):

ATMs are electronic terminals where one has to insert the ATM card and enter the PIN number to withdraw cash, make deposits and transfer funds between accounts. The ATM machine is connected directly to the bank to which it belongs. For example, the SBI ATM is connected to the SBI central server and so on. ATMs can also be used to check the account balance, change the password and pay bills.

a. Direct Deposits:

This lets us to authorize specific deposits to our account on a regular basis. Recurring bills can be paid automatically with direct deposits.

b. Debit card transactions:

Sometimes the ATM card may be a debit card. Purchases can be done and the payments may be made using a debit card. With a debit card payment the money is quickly transferred from our account to the company's account.

c. Electronic check conversion:

Electronic check allows businesses process payments more quickly. Electronic check conversion converts a paper check into an electronic payment.

7.9 PAPERLESS BILL

Paperless Billing is a free service that allows you to receive, view and pay your bills online. The bills are received in an electronic form rather than in a

printed paper format. The paperless billing customers can receive the bills in emails or can also receive them as text messages (SMS) notifications every month. One can pay various utility bills such as electricity bills, telephone bills, mobile bills, mobile top-ups, credit card payments and insurance premium bills online. This facility can be availed through Internet banking. The banks that provides such facilities needs to make tie-ups with the various agencies generating bills, such as the insurance companies, utility companies and government agencies across the country.

There are certain accounts which cannot receive the facility of paperless billing. The prepaid mobile account holders, business, and certain Government and special account types are such examples. To sign up for Paperless Billing, you must first register for Online Services.

Some of the advantages of enrolling to paperless billing are given in the list below.

- View the bills online, anytime and anywhere
- The bills can be received sooner
- They can be downloaded easily and stored in the computer
- Eliminate the paper usage as the bills would be sent via emails and text
- The billing information is secure as the bill is password protected
- Become environment friendly by saving the trees and energy used for printing.

7.10 ELECTRONIC CASH

Electronic cash or e-cash is a new concept in online payment over the Internet. It is one of the alternative forms of payment used in e-commerce. It focuses on replacing cash as the principle payment instrument in payment, although cash is still dominating the payment system. It was originally created by an Amsterdam company, DigiCash, in 1990's.

E-cash is a system that allows the users to make transactions in the real time. Electronic cash or digital cash resembles conventional cash, when the parties exchange electronic tokens that represent value, just as the bank notes and coins determine the nominal value of conventional cash money. These are transmitted over Internet from customer to merchant. The users deposit the money in the bank or provide the credit card. The banks would issue digital tokens for various denominations of cash, which the customers can spend in purchasing things from the merchants' sites. The merchants then deposit those electronic tokens in their bank.

E-cash bears a digital signature for authentication purposes and it can be sent over network either as data or in the form of tokens. It is generally stored in an E-cash account holder's **"wallet"** on the web. An e-wallet is a convenient and secure place to store data related to online identities. When the user needs to make a transaction, the wallet programs communicate with the seller using the wallet program to complete the transaction.
E-cash must have the following four properties

- Monetary value
- Interoperability
- Retrievability
- Security

Examples of e-cash systems are PayPal and Digicash. These systems allow the user to easily transfer money without having to visit a bank and withdraw cash. Consumers find e-cash handy as they avoid paying fees to the bank for using debit card.

A significant disadvantage of electronic cash systems is the need to maintain a large database of the past transactions to prevent double spending. Double spending can be an obstacle for system expansion as it can reduce the scalability of the system.

7.7 ONLINE BANKING

Almost all banks today offer online banking. It is an extension of the bank business on the network. Sometimes it is also called electronic banking or virtual banking. Online banking first started with automatic teller machines (ATM) in the late 1960s.

Online banking has greatly changed the banking industry. With online banking, the customers of a bank can connect their personal computer with the bank's server and carry out the transactions using a web browser. The banks maintain a central database which is web enabled. In India, banks like State Bank of India (SBI) and Housing Development and Finance Corporation (HDFC) first started online banking.

Online banking is when customers perform most of their banking-related functions without visiting the bank, personally. To do so, customers must possess an Internet banking ID and a password provided by the bank in which the individual customer has an account.

Electronic banking is a faster way of performing banking functions. The advantages of online banking system are as follows.

1. **Time saving**

Online banking reduces the time needed to process banking transactions. It allows transferring money between accounts much more quickly. It saves the time to visit to the bank and wait in a queue. These can be one-time transactions or recurring payments at a certain time each month like loan payments.

2. **Direct deposit**

Direct deposit in online banking is having the payments such as paychecks, tax refunds directly deposited into account without the need for a paper check to be printed. In this case, the recipient does not have to go to the bank to deposit the check. One may also pre-authorize direct withdrawals so that recurring bills like insurance premium, membership bills can be automatically paid.

3. **View and manage transactions**

It allows viewing the account history and managing the transactions from anywhere and at any time. It offers 24x7 services. This helps in finding out about any unauthorized transactions more quickly. This can be helpful in resolving the issues.

4. Convenience

Bill payments like electricity bill, phone bill, insurance premiumsetc can be made online with online banking without having to rush to the utility company's bill collection outlets. It helps to avoid delayed payments.

5. Eco-friendly process

Electronic banking is an eco-friendly process as it does not consume volumes of paper like the conventional banking and thus helps to save the environment.

6. Others

Online banking offers several other benefits also like online shopping, ticketing, advance bookings and many others like purchase shares, bonds, mutual funds without the intervention of the financial intermediaries.

Despite of the advantages of using electronic banking, there are a few problems also.

i. Security

One of the biggest problems of online banking is security. It faces various threats such as login details disclosure, dummy websites, computer spy viruses etc. the criminals try to acquire the login details of the customer and use it to steal the money from the account. Phishing is an email fraud method in which legitimate looking emails are sent to the customers in an attempt to reveal the sensitive information from the recipients. Pharming is another security concern in which malicious code is installed on a personal computer or server thereby misdirecting the users to fraudulent websites without their knowledge or consent.

ii. Fraud

Fraud is a common concern as the security features such as a password or a PIN number can be stolen and used without identification.

7.12 CONCEPTS OF EDI

The concept of EDI was first introduced in the 1980's. It formalized the process of exchanging files in a structured and standard format. EDI has gained much popularity in e-commerce because it offers the companies the ability to become more efficient and productive and thereby more competitive.

The manual document exchange involves paper-based processes which are slow, costly and error-prone. An example of such a system in which a customer faxes or mails an order to a supplier who then faxes or mails an invoice back to the customer is shown below.

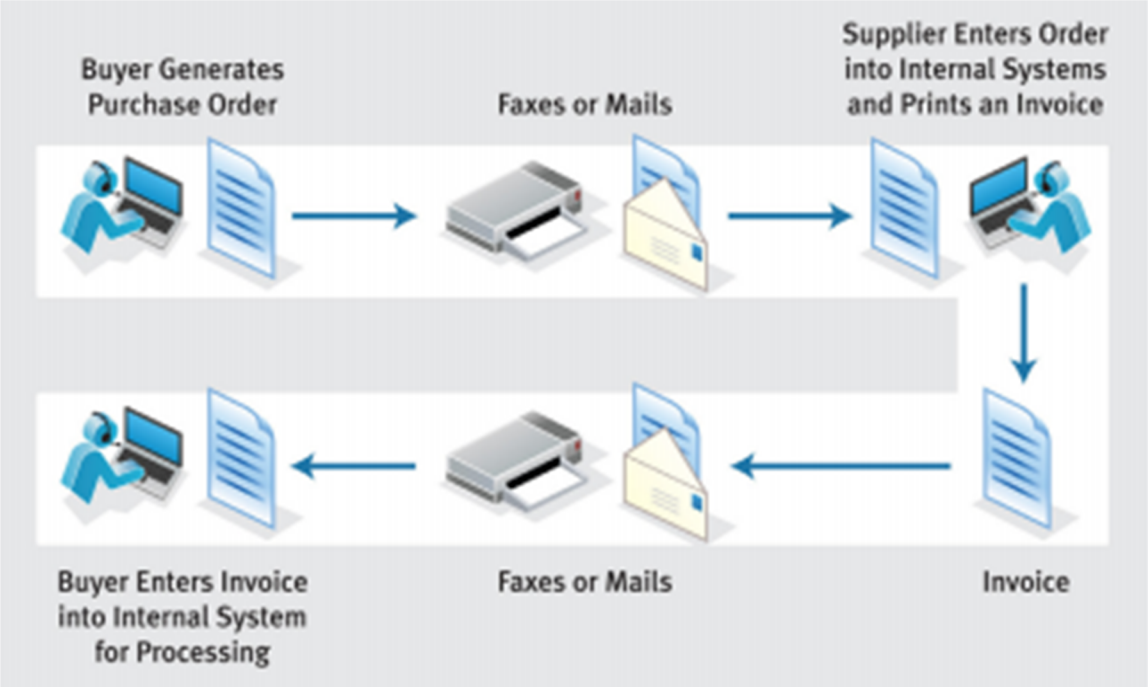

Figure 7.9

This process requires a lot of time, people and paper. Paper-based documents can also be misplaced or lost. In the above process, the supplier after receiving the mail or fax has to enter the details of the order placed into their computer application which again being a manual process might result in errors.

EDI (Electronic Data Interchange) is the computer-to-computer exchange of business documents of information from one trading party to another trading party such as retailers and suppliers, banks and their corporate clients etc.

The documents that are most commonly exchanged are purchase orders and invoices, billing documents, inventory documents, payment documents etc. In fact, today all types of business documents such as retail, banking, logistics, automotive can be exchanged using EDI.

EDI is better than paper-based document transmission because of the following:

1. Improves the information flow, as there is no human interaction or maintenance of paper documents.
2. Reduces the data handling costs involved in sorting, distributing, organizing and searching of a document in a paper-based system
3. Reduces the chances of errors that can occur in the traditional method of using paper.
4. The overall transaction process is fast as information can be exchanged quickly between the interacting parties.

EDI is used not only to exchange business data but it is also used to transfer other information in other fields. For example, in medicine it is used to transfer patient records and laboratory results.

There are several EDI standards which are developed by organizations. The following are the four set of standards that have been defined for EDI.

- ANSI (American National Standard Institute), primarily used in United States.
- EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport), primarily used in Europe and Asia.
- TRADACOMS developed by Article Numbering Association (ANA) and is used in the retail industry in United Kingdom (UK).
- ODETTE (Organization for Data Exchange by Tele Transmission) used in the automotive industry within Europe.

Working of EDI

There are 3 steps involved in sending the EDI documents- Prepare the documents, Translate the documents into EDI format, transmit the EDI document. They are shown in the figure below.

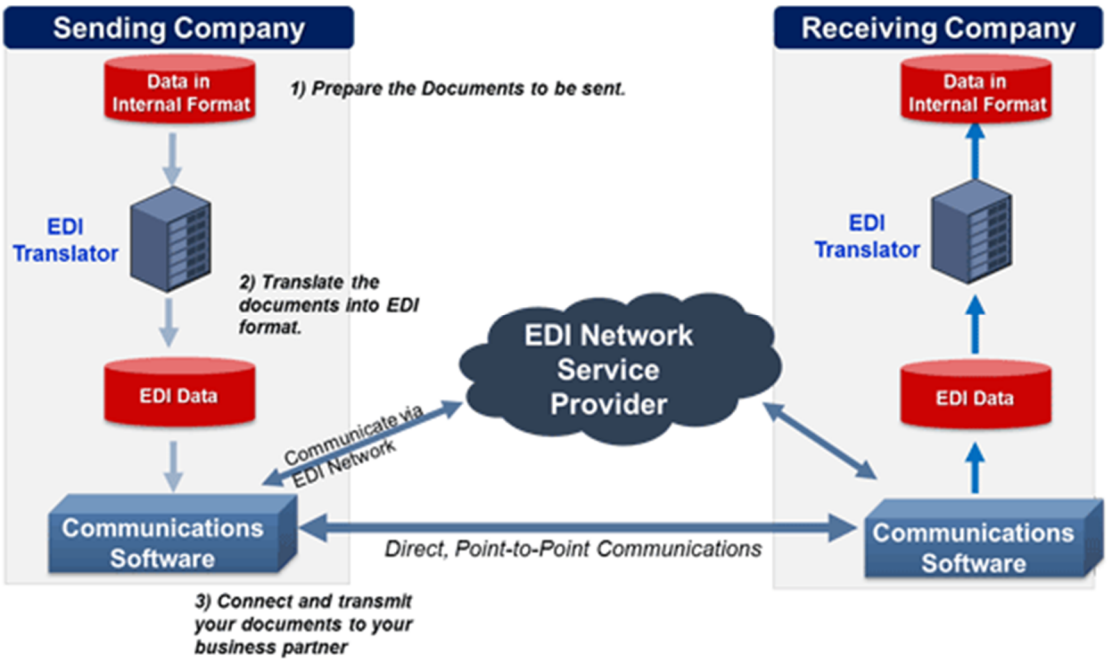

Figure 7.10

The first step involves collecting and organizing the data. The sources of data may include the following.

i. Computer programs that extract data from system databases such as a purchasing system etc.
ii. Computer programs that extract data from spreadsheets
iii. Human data entry via screens.

In the next step, the translator software converts the internal data into the EDI standard format using appropriate segments and data elements. The translation software defines how the internal data is to be mapped to the EDI.

The third step involves transmitting the EDI document. There are two ways to transmit an EDI document. The first is to send it directly to the trading partner via Internet. The second is to use the services provided by an EDI network service provider. In the second case, the document is first sent to the service provider, who then makes it available to the business partner.

7.13 EDI APPLICATION IN BUSINESS

EDI enables the organizations to reduce cost and inefficiency resulting from manual, paper-based systems. It can ensure that the business information is sent securely on time to the other party and also receive data from their trading partners. EDI documents can be tracked in the real time and can also be audited. In today's highly competitive world, the use of B2B technology such as EDI is very important.

EDI I successful in bringing the business partners together by using the Internet.

7.14 LIMITATIONS OF EDI

EDI is a new way of doing business. Although there are many benefits of using EDI, the actual implementation of EDI is less prevalent in small to mid-sized business organizations because of the following limitations of EDI.

1. Expense: The setting and implementation costs associated with EDI system is very high. Organizations also need to conduct weeks of personnel training to run EDI system smoothly.
2. Network Complexity: The need for extensive telecommunications capability is the second major barrier in the implementation of EDI in smaller companies. Setting up of EDI system requires heavy investment in computer network.

CHECK YOUR PROGRESS 3

3.Fill in the blanks

i. _____ has always been the dominant system of transaction. Cash

ii. _____ is an electronic method of making a payment from one bank account to another bank account. Electronic fund transfer

iii. Direct Deposits is a feature of _____. electronic fund transfer

iv. Electronic check conversion converts a _____ into an electronic payment. paper check

v. In online billing system, the bills are received in an _____ rather than in a printed paper format. electronic form

vi. Paperless bill facility can be availed through _____ banking. Internet

vii. Electronic cash or digital cash resembles _____ cash. Conventional

viii. Online banking reduces the _____ needed to process banking transactions. Time

ix. The manual document exchange involves _____ processes which are slow, costly and error-prone. paper-based

x. _____ is the computer-to-computer exchange of business documents of information from one trading party to another trading party. Electronic Data Interchange

7.15 LET US SUM UP

1. 'Payment' refers to value transfer or exchange of money.
2. The exchange of money that is performed through specific electronic means is referred to as electronic payment. Electronic payments that are performed using Internet are called online payments.
3. The credit card brands, Visa and Master, developed the SET (Secure Electronic Transaction) standard to process the card transactions on the Internet.
4. There are four main entities in a SET. They are listed below.
   v. Cardholder (Customer)
   vi. Merchant (Web Server)
   vii. Merchant's Bank (Acquirer)
   viii. Issuer (cardholder's bank).
5. SET protocol relies on cryptography and digital certificate to ensure confidentiality and security.

6. The service that automates and authenticates electronic payments made by the customers to the e-commerce merchants is called Payment Gateway.
7. The different types of Electronic Tokens used are Cash or Real time, Debit or Prepaid and Credit or Postpaid.
8. Smart cards are small, portable pocket-sized plastic cards that contain an embedded computer chip used to store relatively large amount of information and can also transact data.
9. There are two types of smart cards – contact and contactless.
10. Credit card is one of the most common forms of electronic payment for the purchase of goods and services globally.
11. There are two standards to securely use credit cards on the web. They are secure socket layer (SSL) encryption and the Secured Electronic Transaction (SET).
12. A magnetic strip card is a plastic card that has a magnetic stripe on it. Magnetic stripe is also called a magstripe. The stripe is made up of tiny magnetic particles, like iron, in a plastic film.
13. The electronic version of a paper check is the E-check. It can be directly exchanged between the parties. The amount and necessary bank information from the check is captured and sent through the Automated Clearing House (ACH), which transfers the money to the merchant's bank account.
14. The credit/debit card approach in the EPS (Electronic Payment System) means that the money is represented in records in the bank accounts and this information is electronically transferred between the parties over the computer network.
15. Debit card payment is an instant payment system from the customer's account.
16. Traditional payment systems are negotiable instruments such as drafts, bank notes, checks, and credit/debit cards.
17. Electronic fund transfer (EFT) is an electronic method of making a payment from one bank account to another bank account.
18. Paperless Billing is a free service that allows you to receive, view and pay your bills online. The bills are received in an electronic form rather than in a printed paper format.

19. E-cash was originally created by an Amsterdam company, DigiCash, in 1990's.
20. Electronic cash or digital cash resembles conventional cash, when the parties exchange electronic tokens that represent value, just as the bank notes and coins determine the nominal value of conventional cash money.
21. With online banking, the customers of a bank can connect their personal computer with the bank's server and carry out the transactions using a web browser.
22. EDI (Electronic Data Interchange) is the computer-to-computer exchange of business documents of information from one trading party to another trading party such as retailers and suppliers, banks and their corporate clients etc. The documents that are most commonly exchanged are purchase orders and invoices, billing documents, inventory documents, payment documents etc.

7.16 FURTHER READINGS

1. "E-Business", ParagKulkarni, SunitaJahirabadkar, PradipChande, Oxford publication
2. "E-commerce- The cutting edge of business", Kamlesh K Bajaj, Debjani Nag, Tata McGraw-Hill

7.17 ANSWERS TO CHECK YOUR PROGRESS

1. a. Payment system
   b. Customer, merchant
   c. Paperless
   d. Secure Electronic Transaction
   e. Visa and MasterCard
   f. Cryptography
   g. Payment Gateway
   h. Secure order form, Merchant side API

i. fraud.

j. application programming interface

2. a False

b. True

c. True

d False

e. False

f. True

g. True

h. False

i. True

j. True

3 i. Cash

ii. Electronic fund transfer

iii. electronic fund transfer

i. paper check

ii. electronic form

iii. Internet

iv. Conventional

v. Time

vi. Paper-based

vii. Electronic Data Interchange

7.18 MODEL QUESTIONS

1. Describe in detail the online payment procedure in credit card system.
2. Compare credit card and debit card payments.
3. Explain the payment sequence in an e-ck system.
4. What are the advantages of EPS over the traditional payment system?
5. Describe some EFT services
6. Compare EDI with paper-based document transmission

****

UNIT 8: E- GOVERNANCE FOR INDIA AND LAW

UNIT STRUCTURE

8.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- learn about electronic governance in India
- learn about the cyber laws in India that deals with cyber space activities
- learn what is cybercrime and the different types of cyber crimes
- describe the Indian Customs EDI system

8.2 INTRODUCTION

Information technology is one of the forces in India's growth. The government of India has taken a lead in the increased adoption of IT-based products and solutions in the country. The increasing dependence of the people and the government on Information Technology has also led to rising threats to cyber security through cyber crimes, cyber attacks and cyber wars. The word 'cyber' was first coined by William Gipson in his novel 'Neuromancer' in the year 1984.

The International Telecommunication Union defines cyber security as "A collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that can be used to protect the cyber environment, including organizations' and user's assets".

8.3 E-GOVERNANCE OF INDIA

Electronic governance in public administration means rendering of government services and information to the public using the electronic means. This new system has brought a revolution in the quality of service delivered to the citizens. The electronic governance will help in low cost, time saving, efficient and transparent working of the government department, reduction in corruption and improved attitude behavior and job handling capacity of the dealing personnel. It offers better office and record management. Thus it focuses mainly on improving the administrative efficiency and reducing the corruption at the administrative level of governing.

The two terms 'E-government' and 'E-governance' are independent of each other although sometimes they are used interchangeably. E-government uses Information and Communication Technology (ICT) to promote an efficient and cost effective government, facilitate better government services and provide transparency to governing processes by making the government accountable to the citizens. However, E-governance is the use of ICT by the government, society and public institutions to engage the citizens to promote their greater

participation in governing these institutions. Thus e-government is a subset of e-governance.

E-Governance in India has evolved from computerization of the government departments. The Government of India first approved the National E-Governance Action Plan for implementation during the year 2003-2007. It is an attempt to lay the foundation and provide impetus for long term growth of e-governance within the country. Apart from the action plan other measures have also been introduced. The latest being the adoption of the IT Act, 2000 to provide legal framework to facilitate e-transaction. The main aim of the act is to prevent computer crimes and make the electronic filling possible.

Rules of Electronic Governance

The Information Technology Act provides a legal recognition for the electronic records. It means that the government departments and offices can accept the documents in the electronic form and they are valid legal documents. Digital signatures has also been given legal recognition by the IT act, which in turn means that any document that is signed digitally will be treated as valid and authenticated electronic records. The government applications and forms can be filled up through electronic means. The government departments can also issue or grant any license and permissions through electronic means.

Examples

e-filling related income tax ---- https://incometaxindiaefiling.go.in

e-filling for patent application ---- https://ipindiaonline.gov.in/on_line

8.4 CYBER LAW IN INDIA

The term ‘Cyber Law’ is used to describe the legal issues related to the uses of communication technology, particularly the “cyberspace”. Cyber space is a wide term that includes computers, Internet, websites, emails and even the electronic

devices such as the cell phones, ATM machines etc. The laws are approved by the government and violation of the rules could lead to government action such as imprisonment or fine or an order to pay the compensation.

Cyber law relates to mainly the following:

- Cyber crimes
- Electronic and Digital Signatures
- Intellectual property
- Data protection and privacy.

The new age cyber crimes are dealt with the Information Technology Act 2000. This act amended by the IT (Amendment) Act 2008, is the foundation of the Cyber Law in India. This law provides for the civil remedies for the cyber torts and penal liabilities for computer crimes. This act applies to cyber offences that is committed inside or outside India by any person irrespective of his nationality provided it is committed against a computer system located in India.

The IT Amendment Act 2008 was placed in the Parliament towards the end of 2008. The Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.
It has a separate chapter XI entitled “Offences” in which different cyber crimes have been declared as penal offences.

CHECK YOUR PROGRESS 1

1. Fill in the blanks:

a. _____ focuses mainly on improving the administrative efficiency and reducing the corruption at the administrative level of governing. E-governance

b. E-government uses _____ to promote an efficient and cost effective government, facilitate better government services and provide transparency to governing processes by making the government accountable to the citizens. Information and Communication Technology (ICT)

c. The Government of India first approved the _____ for implementation during the year 2003-2007. National E-Governance Action Plan
d. In e-governance, the government departments can also issue or grant any license and permissions through_____. electronic means
e. _____ is used to describe the legal issues related to the uses of communication technology, particularly the "cyberspace". Cyber law

8.5 COMPUTER CRIME

Cyber crime is a general term that refers to all the criminal activities done using computers, the Internet and the World Wide Web. In cyber or computer crime, the unlawful acts use a computer either as a tool or a target or may be as both. These types of cyber crimes can involve criminal activities such as fraud, theft, forgery etc. These crimes are subject to the Indian Penal Code. Cyber crime includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts.

The word 'cyber crime' or 'computer crime' has not been defined in the Indian law. The Indian Penal Code does not use the term 'cyber crime' even after its amendment by the IT (Amendment) Act 2008, the Indian Cyber Law. However, 'Cyber Security' is defined under section 2(b). Computer crimes are the crimes that involvethe computer specially using the Internet. Computer crimes may be caused due to

a. Lack of proper computer security
b. Low equipment cost
c. Lack of legal awareness
d. Lack of awareness among the victims and the accused.
e. Tremendous growth of E commerce and online share trading
f. Global connectivity

8.5.1 Types of Crime

Some of the common cyber crimes are given as follows:

1. **Hacking**

Hacking means unauthorized access to a computer system, programs, data and resources. This is a type of crime where a person's computer is broken so as to access his personal or sensitive information. In hacking, a person may not even be aware that his computer has been hacked, that is accessed by somebody else.

2. **Email spoofing**

Email spoofing means sending an email to another person in a way that it appears that the mail was sent by someone else. That is, a spoof email appears to originate from one source but actually it has been sent from another source. It is usually done to spread unsolicited mails and also viruses. In email spoofing, the hacker changes the sender address and the other parts of the email header so as to make it appear as though it has been originated from a source other than its actual source. This is also termed as email forging.

Under IT(Amendment) Act 2008 section 66-D and section 417, 419 and 465 of the Indian Penal Code are applicable to such offences.

3. **Spreading viruses and worms**

Viruses are malicious programs or software that attach themselves to a computer or a file and then spread to other files on the computer or other computers on a network. They may corrupt or delete the data on the computer. They are easily spread as attachments in email messages. Downloading information from the Internet also spreads viruses. Viruses can be classified as file infectors and boot sector infectors. Viruses can ruin the system and render it unusable till the operating system is re-installed in the system. They can replicate themselves and move to other potential victims.

Worms, unlike viruses, do not need a host to attach themselves to. They make functional copies of themselves and continue till they use up all the available space on the computer.

According to section 43 (c) of the IT Act, if any person introduces computer virus into the computer system or computer network without permission of the owner he shall be liable to pay the damages by compensation. For example, sending a virus infected file to a person and thereby introducing the virus in his system without his consent would make one liable under section 43(c). If such an act is done fraudulently then under section 66, he may be imprisoned for a term which may extend to 3 years or a fine which may extend to rupees 5 lakh or may be both.

4. Data theft

This crime occurs when a person violates the copyrights and downloads software, music, games, music etc. There are laws to prevent people from illegal downloading.

Data theft is dealt with section 43(b) of the IT Act. The wrongdoer can be imprisoned for a term which may extend to three years or fine which may extend to 5 years or both, under section 66.

5. Cyber stalking:

Cyber stalking is a kind of online harassment wherein the victim is bombarded with online messages and messages. The stalkers in this case knows who the victim is and uses Internet to stalk. It usually occurs with women who are stalked by men or children who are stalked by pedophiles. When children are involved it is called cyber bullying.

The minors use the instant messengers, email, social networking sites, website, interactive games etc to frighten, embarrass or harass another minor. Section 66A provides cover for cyber stalking, threat mails, phishing mails, SMS etc.

6. Cyber terrorism

Cyber terrorism is the convergence of terrorism and cyber space. It is a politically motivated attack against information, computer systems, programs and data which results in violence. It is used to cover attacks like 26/11 in which the terrorist accessed the hotel computers to gather information about the US and UK citizensstaying there and selectively choose them as targets. The 11/9 attack was also designed and planned using Internet.

Section 66 F of the IT Act deals with cyber terrorism. The punishment for cyber terrorism is imprisonment which may extend to imprisonment for life.

7. Cyber pornography

It refers to stimulating sexual or other erotic activity over the Internet. Section 67 of the IT Act is the most serious law dealing with this type of cyber crime. Depending upon content, the section 67A and 67B (child pornography) may also be applicable. Section 66E deals with punishment for violation of privacy. The acts like hiding cameras in changing rooms, hotel rooms etc is a punishable offence with jail upto 3 years. Other laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code.

8. Email fraud

The fraud committed with the help of an email is called email fraud. Common example is the lottery fraud wherein an email informs a user that he has won a huge sum of money in a lottery. Actually there is no lottery and no prize.

The sections attracted for such are Sec 66C and 66D of the IT Act and the relevant provisions in the Indian Penal Code, Section 415(cheating) and Section 420(cheating and dishonestly inducing delivery of property).

9. Spamming

The receiving of a large number of unsolicited emails is called as spam. Generally the commercial companies send these as an advertisement of their products and services. Section 43(c) (e) (f) of the IT Act deals with the problem of spam.

10. Denial of Service attacks

This type of attacks involves flooding a computer with more requests than it can handle.They are caused by programs that repeatedly request information from a computer until that computer is unable to answer any more request.

These are actually bandwidth consumption attacks or resource starvation attacks. It causes the computer (example, a web server) to crash. Another variation to the denial of service attack is known as Distributed Denial of Service (DDoS) attack where the perpetrators are many and are geographically widespread.

The remedy is civil (Sec 43(f) of the IT Act) and criminal (Sec 66).

11. Web Jacking

In web jacking, a hacker forcefully takes up the control of a website.The owner loses his control on the website after that. In US a case was reported where a children website was web jacked. The website had a portion 'How to play with gold fish' which the hackers changed into 'How to play with piranhas'. Piranhas are dangerous fish.The website was a hobby website. The children followed the instructions to play with piranhas, following which they got seriously injured.

Web jacking, in India, is punishable under section 383 of the Indian penal Code (extortion).

12. Identity theft

In this the criminal use Internet to steal personal information from other users. This is generally done through *phishing* and *pharming*. These methods lure the users to fake websites where they are asked to enter personal information. This includes login information such as usernames and passwords, phone numbers, credit card numbers, bank account information etc.

CHECK YOUR PROGRESS 2

2. Say True or False:

a. Allowing a person to have access to a computer system, programs, data and resources is called hacking.
b. A spoof email appears to originate from one source but actually it has been sent from another source.
c. Viruses cannot be spread as attachments in email messages.
d. Data theft is dealt with section 43(b) of the IT Act.
e. Cyber bullying is a type of stalking.
f. Section 66A provides cover for cyber stalking, threat mails, phishing mails, SMS.

g. Cyber Terrorism is not related to computers.
h. The most serious law dealing with cyber pornography is Section 67 of the IT Act.
i. Downloading illegal music files is not under Cyber Crime.
j. Global connectivity may be one of the reason for increasing number of crimes.

8.6 INDIAN CUSTOM EDI SYSTEM

The Indian Custom EDI system (ICES) has started a new age of paperless trade in the country. Its aim was to improve the way the businesses conduct their business. It allows the trading communities of our country to exchange document electronically with the Customs and other government agencies. The documents can be prepared and submitted using either the Electronic Data Interchange or Service centre. It is developed for better management of the Custom activities.

The system is the result of a study conducted by the National Informatics Centre and central Board of Excise and Customs in December, 1992. The pilot project was launched in the year 1994-95 at the Delhi Customs House which included Electronic Data Interchange (EDI) as a key element for electronically connecting the trading companies involved in International trade with the customs house.

The Indian Custom EDI system consists of two main sub-systems.

a. Indian Customs EDI system/Imports (ICES/I)
b. Indian Customs EDI system/Export (ICES/E)

The Indian Customs provide a downloadable Remote EDI System (RES). The Importers/Exporters and the Custom House agents can use this graphical user interface based packageto prepare the documents in the required format. The RES is a user-friendly software implemented using Visual Basic/Oracle8. It has been developed by NIC as a component of the ICES. These documents are then transmitted over the Internet using the NIC server for submission at the Customs house for further processing. When the documents are received, they are loaded

to the ICES after proper validation checks. If any error found on validation, they are reported to the Importer/Exporter/Custom House Agents through EDI or at the Service Centre.

The main objectives of ICES by customs are

1. Quick response to trade needs
2. Computerization of customs related functions like import/export, goods imported against export promotion schemes, monitoring of export promotion schemes etc.
3. Reduce trade interaction with government agencies.
4. Provide information retrieval from other customs location to have a uniformity in assessment and valuation.
5. Provide quick and correct information on import/export statistics.

Some of the main features of Indian Customs EDI system are as follows:

- **Management and Control**:
    - The progress of the processing of the documents by the custom officers can be monitored and thereby provide the necessary help required in the process.
    - The number of documents that are cleared at each stage can also be monitored.
- **Security**:
    - Security at all levels of access to the system is provided by the ICES. The system keeps a track of all the transactions carried out by the system.
- **Help**:
    - The system provides a powerful help feature to help the assessing officers in their work.

There are many advantages of the computerization of the Indian Customs system. They are as given below.

- ✓ Time and Cost saving as with computerized system there is a reduction in the need to prepare, handle, store and deliver the customs documentation.
- ✓ Quick access to the information and the transparency of the customs processes has increased the level of fairness.
- ✓ Proper compliance track results in faster clearance and less intrusive verification procedures.
- ✓ Higher efficiency. Reduction in manual administrative processes leads to fewer errors and no duplication.
- ✓ Data accuracy
- ✓ Customer satisfaction

8.6.1 Service Centre

The Customs and Central Excise departments also run service centers for Importers/Exporters and the Custom House agents who do not have access to Internet. These people can prepare their documents electronically and submit the same at the service centre for further processing. The service center software package developed by NIC runs on a powerful Sun machine using Oracle 7.0 and allows the data entry, modifications and submissions.

The Service Centre provides a host of services to the external stakeholders like the Customs House Agents (CHA), Shipping Agent (SA), Importer/Exporter etc. The service centre acts as the interface between the service-seekers and Customs. The data entry and processing personnel at the service centreuse the ICES Service Centre to process the user requests.

Some of the facilities provided at the service centre are:

1. Job submission and
2. Checklist generation
3. Query printout and reply entry
4. Document status enquiry
5. Printing of processed documents etc

Some of the important documents that are processed through the service centre are listed below.

a. Bill of Entry
b. Shipping bill
c. Amendment request
d. Query reply
e. License etc

8.6.2 Import

The bill of entry can be filed by the importer at the service center. They are required to also submit a signed declaration in a prescribed format along with a copy of their invoice and packaging list. The documents can also be filed through the RES. After the data entry at the service center, the data is checked and a check list is generated. This has to be verified by the Importer/Custom House Agent (CHA). If there is any discrepancy, the list is corrected and the signed list is submitted at the service center. In case of the Remote EDI System users, the system validates the data and if there is no discrepancy then the system accepts it. The RES users receive an acknowledgement on acceptance. If error is detected, a message is sent back to the user.

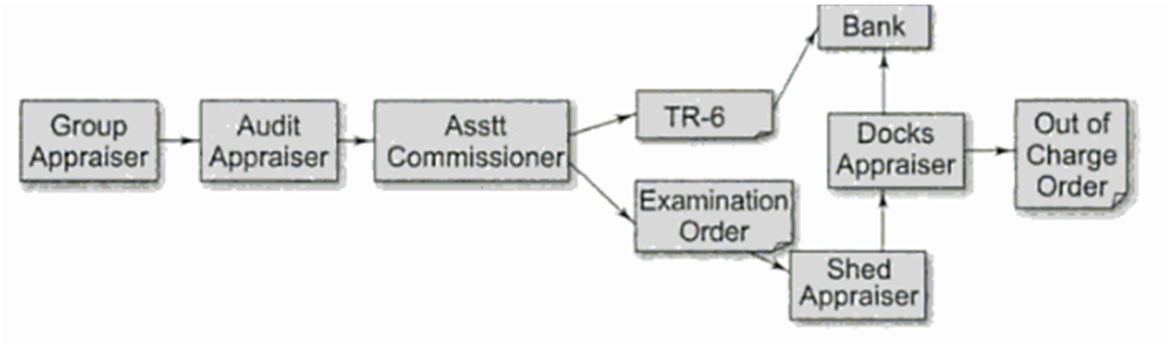

Figure 8.1 Workflow process at the Indian Customs for Import

The above figure describes the workflow process for the movement of the Bill of Entry. The bills that are accepted moves to the respective group appraiser. The

group appraiser then access it and forwards it to the audit appraiser. When the audit is complete, the bill of entry is sent to the assistant commissioner of the group. He then approves the appraisal and the audit assessment. The payment advice form TR-6 and the examination order are printed at the service center. The importer/CHA is required to pay the duty at the designated bank using the TR-6 form. The work flow process then marks the bill of entry to the appraiser (docks). The importer/CHA also approaches the shed appraiser and presents a copy of the bill of entry along with duly paid receipt and other documents including the invoice, packing list etc. for examination of the goods. After examining the goods, the shed appraiser enters the examination information into the system. On completion of the examination of the goods, the appraiser (docks) gives the “Out of Charge” order on the system. The system prints two copies of the bill of entry for the importer and the exchange control. The dock officers file the reports and enters them in the system.

8.6.3 Export

The ICES Export system can be used only by the registered users. So before filing any export shipping bill, all exporters and CHAs are required to register with the Customs EDI system. In order to register they are to provide their IEC code number, CHA license number and authorized dealer code number of the bank through which the exports are to be realized. The registered users can then file the shipping bill for export using the prescribed formatduly signed by the exporter or his CHA,at the service center. He also has to present a copy of the invoice and the packing list. After the data entry at the service center, a check list is generated. The exporter/ CHA have to verify the data entered. If there is any discrepancy in the entered data, they have to inform the service center operators for making the necessary correction in the entered data. Once the data is correctly entered, the system will generate a shipping bill which is automatically processed by the system on the basis of the declaration made by the exporters. However, the following shipping bills are accessed by the Assistant Commissioner (Export).

(a) Shipping Bills where the FOB value is more than Rs. 10 Lakhs.

(b) Shipping Bills relating to free trade samples whose value is more than Rs.20,000/-

(c) Drawback Shipping Bills where drawback amount is more than Rs. 1 Lakh.

During the processing if any query is raised, then the exporter/CHA has to reply the queries through the service centers.

The exporter/CHA is required to produce a checklist along with the original documents such as invoice, packing list etc to the customs officer. After the processing is over, the goods are examined at the docks. If everything is in order after examination of the goods and scrutiny of the documents, the appraiser issues a “Let Export” order to the ICES/E. Then the printout of the shipping bill is generated. The examination report printed on the shipping bill is to be signed by the appraiser, the examiner and the exporter. It also includes the name and license number of the CHA.

CHECK YOUR PROGRESS 3

Fill in the blanks.

a. The aim of _____ was to improve the way the businesses conduct their business.
b. Remote EDI System is a _____ based package to prepare the customs’ documents in the required format.
c. The service center software package developed by NIC runs on a powerful Sun machine using _____.
d. After the data entry at the service center for import, the data is checked and a check list is generated which is verified by the _____ .
e. The RES is a user-friendly software implemented using _____.

f. The pilot project of Indian Custom EDI system was launched in the year _____ at the Delhi Customs House.
g. The Remote EDI system has been developed by _____ as a component of the ICES.
h. The shipping bill of the ICES Export is to be signed by the appraiser, the_____ and the_____.
i. The ICES Export system can be used only by the _____users.
j. When examination of the goods is over for import , the appraiser(docks) gives the _____ order on the system.

8.7 LET US SUM UP

1. Electronic governance in public administration means rendering of government services and information to the public using the electronic means.
2. E-Governance in India has evolved from computerization of the government departments.
3. 'Cyber Law' is used to describe the legal issues related to the uses of communication technology, particularly the "cyberspace".
4. The laws are approved by the government and violation of the rules could lead to government action such as imprisonment or fine or an order to pay the compensation.
5. Cyber crime is a general term that refers to all the criminal activities done using computers, the Internet and the World Wide Web.
6. Hacking means unauthorized access to a computer system, programs, data and resources.
7. Email spoofing means sending an email to another person in a way that it appears that the mail was sent by someone else. This is also termed as email forging.
8. Viruses can be classified as file infectors and boot sector infectors.

9. If any person introduces computer virus into the computer system or computer network without permission of the owner he shall be liable to pay the damages by compensation.
10. Cyber stalking is a kind of online harassment wherein the victim is bombarded with online messages and messages.
11. When children are involved in cyber stalking it is called cyber bullying.
12. Section 66A provides cover for cyber stalking, threat mails, phishing mails, SMS etc.
13. Cyber Terrorism is a politically motivated attack against information, computer systems, programs and data which results in violence.
14. Section 67 of the IT Act is the most serious law dealing with cyber pornography.
15. The acts like hiding cameras in changing rooms, hotel rooms etc is a punishable offence with jail up to 3 years.
16. Denial of service attacks involves flooding a computer with more requests than it can handle.
17. Another variation to the denial of service attack is known as Distributed Denial of Service (DDoS) attack where the perpetrators are many and are geographically widespread.
18. Identity theft is generally done through *phishing* and *pharming*.
19. The Indian Custom EDI system (ICES)'s aim was to improve the way the businesses conduct their business.
20. ICES accepts the electronic documents entered by the trading partners.
21. The Indian Custom EDI system consists of two main sub-systems - Indian Customs EDI system/Imports (ICES/I), Indian Customs EDI system/Export (ICES/E)
22. The Indian Customs provide a downloadable Remote EDI System (RES) to electronically prepare the documents by the trading partners.
23. The Customs and Central Excise departments also run service centers for Importers/Exporters and the Custom House agents who do not have access to Internet.

8.8 FURTHER READINGS

1. “Electronic Commerce” , Jeffrey F Rayport and Bharat Bhasker, Tata McGraw Hill.

2. “IPR and Cyber Space – Indian Perspective”, RohasNagpal

3. Indian Customs EDI System ICES/Imports Version 1.5 by National Informatics Centre, Ministry of Communication & Information Technology.

8.9 ANSWERS TO CHECK YOUR PROGRESS

1. a. E-governance
   b. Information and Communication Technology (ICT)
   c. National E-Governance Action Plan
   d. electronic means
   e. Cyber law
2. a. False, b. True, c. false, d. True, e. True, f. True, g. False, h. True, i. False,j.True
3. a. Indian Custom EDI system (ICES), b. Graphical User Interface, c. Oracle 7.0, d. Importer/Custom House Agent (CHA), e. Visual Basic /Oracle8, f.1994-95, g. National Informatics Centre, h. Examiner, exporter, i. Registered, j. Out of Charge

8.10 MODEL QUESTIONS

1. What is e-Governance?
2. What is meant by cyber crime and Cyber Law? Explain some computer crimes and the related law in India to deal with those types of crimes.
3. Explain the Denial of Service attack.
4. How does the Indian Custom EDI System does helps in International trading?

*****