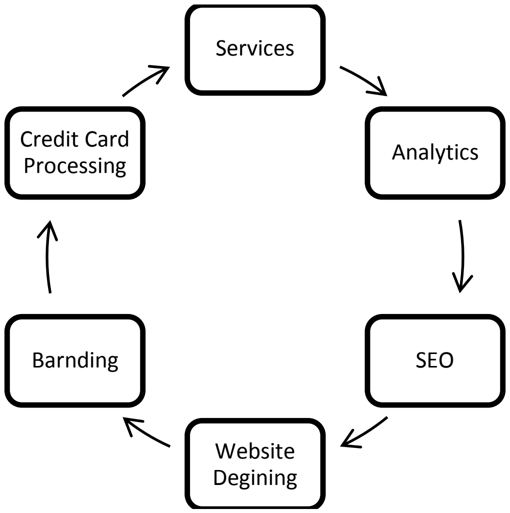
MCA-303

E-Commerce



VARDHMAN MAHAVEER OPEN UNIVERSITY
KOTA

www.vmou.ac.in

MCA-303

Vardhman Mahaveer Open University, Kota

E-Commerce

Course Development Committee

Chair Person

Prof. Ashok Sharma
Vice-Chancellor
Vardhman Mahaveer Open University, Kota

Prof. L.R. Gurjar
Director Academic
Vardhman Mahaveer Open University, Kota

Convener and Members

Convener

Neeraj Arora
Assistant Professor, Computer Science
School of Science and Technology,
Vardhman Mahaveer Open University, Kota.

Members

1. **Prof. (Dr.) Reena Dadich**
   Professor and Head (CS)
   University of Kota, Kota
2. **Prof. (Dr.) N.K. Joshi**
   Professor (CS) and Director, MIMT, Kota
3. **Dr. Harish Sharma**
   Associate Professor, CSE Deptt.
   Rajasthan Technical University, Kota
4. **Mr. Abhishek Nagar,**
   Programmer Officer, VMOU, Kota
5. **Dr. Anuradha Dubey**
   Deputy Director
   School of Science &Technology
   Vardhman Mahaveer Open University, Kota

Editor & Unit Writers **MCA-303: E-Commerce**

Editor

Prof. (Dr.) Nemi Chand Barwar
Professor, Computer Science and Engineering,
M.B.M. Engineering College, Jodhpur

Unit Writers	***Units***
Mr. Indiver Purohit Professor, Computer Science and Engineering, M.B.M. Engineering College, Jodhpur.	**1, 2**
Mr. Anil Kumar Sharma Assistant Professor, Department of CS, Govt.Women Engg. College, Ajmer.	**3, 8**
Mr. Piyush Vyas Associate Professor & Department Proctor, ECE Department, J.I.E.T., Jodhpur.	**4, 6, 7, 9, 11, 12**
Mr. Parth Vidyarthi Asst. Professor (Computer Science & Engg. Deptt),Career Point University, Kota	**5**
Mr. Sanjay Kumar Anand Assistant Professor, Department of Computer Science, Central University of Rajasthan, Kishangarh, Ajmer	**10**
Mr. Yogesh Sharma Retd. Associate Professor of Law, Vardhman Mahaveer Open University, Kota	**13**

Academic and Administrative Management

Prof. Ashok Sharma Vice-Chancellor Vardhman Mahaveer Open University, Kota	**Prof. L.R. Gurjar** Director (Academic) Vardhman Mahaveer Open University, Kota
Dr. Shiv Kumar Mishra Director (MP&D) Vardhman Mahaveer Open University, Kota	

Print: 2018 **ISBN: : 978-81-8496-642-8**

All Right reserved. No part of this Book may be reproduced in any form by mimeograph or any other means without permission in writing from Vardhman Mahaveer Open University, Kota.

Printed and Published on behalf of the Registrar, Vardhman Mahaveer Open University, Kota.
Printed by :

MCA-303

Vardhman Mahaveer Open University, Kota

E-Commerce

Contents

Preface

The present book entitled "E-Commerce" has been designed so as to cover the unit-wise syllabus of MCA-303 course for MCA 3rd Year students of Vardhman Mahaveer Open University, Kota.

E-commerce is a catchy term for any commercial transaction that is conducted electronically on the internet, be it from a mobile device, tablet or desktop. Most commonly, E-commerce is used to refer to a consumer purchasing a product online and having it shipped to them directly, but can also include the consumer purchase of services, business to business transactions for goods or services, online auctions, or the purchase of digital goods, such as streaming movies or video games.

This book provides the detailed overview of E-commerce. This book starts with comparison of E-commerce with traditional commerce, various E-commerce models, Mobile commerce, Security and threads associated with E-Commerce, tools to cope threads against E-commerce. At the end we will discuss some fundamental of Internet and Extranet and also some legal issues related to E-commerce in India.

Each unit begins with objectives, introduction and principles together with illustrative and other descriptive material .The illustrative examples serve to illustrate and amplify the theory of computation. The units have been written by various experts in the field. We believe that this book is well suited to self-learning. The text is written in a logical sequence and is beneficial for students. The concise and sequential nature of the book makes it easier to learn. Although we have made all efforts to make the text error free, yet errors may remain in the text. We shall be thankful to the students and teachers alike if they point these out to us. Any further comments and suggestions for future improvement are welcome and will be most gratefully acknowledged.

UNIT-1

Introduction to Electronic Commerce

Structure of the Unit

1.0 Objective

In this chapter we shall focus upon the following topics

- Files and its structure in system
- File types
- File Permission
- Links of files
- File size and space with date and time

1.1 Motivation

eCommerce is a catchy term for any commercial transaction that is conducted electronically on the internet, be it from a mobile device, tablet or desktop. Most commonly, eCommerce is used to refer to a consumer purchasing a product online and having it shipped to them directly, but can also include the consumer purchase of services, business to business transactions for goods or services, online auctions, or the purchase of digital goods, such as streaming movies or video games.

Before eCommerce became a part of our daily lives, most businesses were in competition within their industry and specific geographic location. For example, if you needed to purchase a new shirt, chances are you'd be selecting from the retail options available within a few miles of your home or work. These retail stores wouldn't have considered themselves in competition with stores across state lines. Now, however, the internet is blurring those boundaries and introducing avenues of competition that previously did not exist.

Components of eCommerce :-

The lure of starting your own eCommerce business (or adding eCommerce on top of your traditional commerce foundation) can be incredibly attractive. Coupled with the hundreds of third party services providers that tout the "ease and simplicity" of building an eCommerce store on their platforms (such as Shopify and Wix), you may feel ready to jump in with both feet! But before you proceed, you should be aware of the components that go into not only setting up your online store, but processing payments, fulfilling orders, and providing customer support (just to name a few).

Product or Service:

The most basic component to any eCommerce system is the product being offered. Your product (or products, a la Amazon) can be anything from televisions to filing cabinets, prom dresses to dinnerware – the opportunities are endless. As we mentioned before, eCommerce is not limited to physical goods, but can be extended to allowing customers to select and purchase your service plans online, purchase digital goods, such as pre-recorded webinars, or grant access to member-only features of your website.

When considering what you will offer for sale through your eCommerce system, you must determine how you will obtain the products that you are selling. Are you making your products by hand? Will you be purchasing your products in bulk from the manufacturer? Will you need to arrange an agreement with a distributor? Do you have blind drop ship arrangements with producers?

Depending on what you are selling and how you plan on procuring it, there may be additional considerations such as legal contracts, affiliate agreements, packaging needs, labelling requirements, UPC or barcode generation, federal or state level regulations, and even resell agreements.

If your eCommerce is a new business, you may also need to think about your inventory and product storage. Will your products be delivered on a truck requiring a loading dock for unloading? Are they particularly large or will they require certain temperature considerations during storage? Are they fragile, perishable or living? Will they have a shelf life? How will you track inventory you have in stock, versus what is in delivery? What are the turnaround times for purchasing new product and having it available for sale through your eCommerce?

When it comes to product, packaging, inventory and storage, there are a wide variety of scenarios that may apply to your situation. Although we at Grid have experience in each of these situations, the nuances of each are too exhaustive to cover in this article. If you are preparing your eCommerce solution and need assistance in any of the topics being discussed in this article, we encourage you to reach out to us for more direct and specific support.

Website:

Now that you've identified what you are (or will be) selling, and how you will receive and store it, the next step is to set up the place where you will connect with your customers and enable the transaction to happen – your website.

As we mentioned earlier, there are quite a few third party services that provide "out of the box" online eCommerce systems. These solutions can be great for simple eCommerce stores, such as those with only a few products, those with products that do not have many variants (such as size or color options), or those that don't plan to process too many orders. The benefit to these platforms is they allow you to get up and running fairly quickly: you sign up for a monthly plan, choose a design template, and connect it to your payment processor (which we will cover below), put up a few products and you are off and running!

But, as most of our clients who started with one of these solutions have found, most businesses that plan to really focus on their eCommerce business find themselves outgrowing the capabilities of the platform fairly quickly, and need to move on to a more robust, extendible, or even customizable solution. Just as every business is different from another, so, too, are their eCommerce needs.

Credit Card Processing:

One of the most headache-inducing parts of eCommerce used to be navigating the waters of credit card processing, gateways, contracts and monthly fees. But as more businesses have pursued eCommerce solutions, the demand for an "easier" approach to accepting credit cards online has grown exponentially. Businesses were clamoring for a credit card acceptance system that did away with antiquated fee structures, contractual requirements, and penalties for accepting credit cards that weren't "in hand" to be run through a swipe-style machine.

A number of new credit card processors have entered this field to respond to the demand, making accepting credit cards online easier, safer, and more cost efficient. At Grid, we regularly recommend Stripe to our clients (depending on their needs, of course) to accept payments or donations. If Stripe doesn't meet your needs, you may also consider Square or Google Wallet.

On the other side of the spectrum, most eCommerce systems readily connect to Paypal for accepting payments. We, however, would strong advice against using Paypal for any business transactions since although they act like a bank they are not classified (and thus not regulated) as one. They are not required to maintain any of the security, customer service, or dispute resolution services that typical banks are held to, which can result in sudden and inexplicable freezing of your account with no actual recourse.

Marketing and Traffic:

With your online store up and running, you may be inclined to kick back and wait for the orders to come rolling in. We hate to spoil your moment of zen, but an eCommerce website is not a "build it and they will come" scenario. Remember how we talked about the internet opening up new lines of competition for traditional commerce businesses? Every online business is in competition with every other online business offering the same or similar products or services – so the real work in your eCommerce website has just begun!

When it comes to marketing your eCommerce system, there is an almost infinite number of marketing strategies that could prove successful in driving traffic (and thus sales) to your website. The marketing campaign you embark on should be designed around informed decision-making about your product, demographics and messaging. But the important takeaway here is that you must be doing something to get the word out, whether that's a loyalty program, social media campaign, email newsletters, deals of the day, free samples, etc.

1.2 Brief History of E Commerce

Development of EC applications started in the early 1970s with electronic funds transfer (EFT), which refers to the computer-based systems used to perform financial transactions electronically. However, the use of these applications was limited to financial institutes, large corporations, and some daring businesses.

Electronic data interchange (EDI) was then developed in the late 1970s to improve the limitation of EFT. EDI enlarged the pool of participating company from manufacturers, retailers, services, and others. Such systems were called Interorganizational System (IOS).

An Interorganizational System (IOS) allows the flow of information to be automated between organizations to reach a desired supply-chain management system, which enables the development of competitive organizations.

From the 1990s onwards, electronic commerce would additionally include enterprise resource planning systems (ERP), data mining and data warehousing.

The term 'electronic commerce' was coined in the early 1990s when Internet became commercialized and users began flocking to participate in the World Wide Web. EC applications were then rapidly expanded.

Possibly EC is introduced from the Telephone Exchange Office. The earliest

example of many-to-many EC in physical goods was the Boston Computer Exchange, a marketplace for used computers launched in 1982. The first online information marketplace, including online consulting, was likely the American Information Exchange, another pre-Internet online system introduced in 1991.

1.3 Advantages and Disadvantages

Advantages:-

E-Commerce advantages can be broadly classified in three major categories:

- Advantages to Organizations
- Advantages to Consumers
- Advantages to Society

Advantages to Organizations:

- Using E-Commerce, organization can expand their market to national and international markets with minimum capital investment. An organization can easily locate more customers, best suppliers and suitable business partners across the globe.
- E-Commerce helps organization to reduce the cost to create process, distribute, retrieve and manage the paper based information by digitizing the information.
- E-commerce improves the brand image of the company.
- E-commerce helps organization to provide better customer services.
- E-Commerce helps to simplify the business processes and make them faster and efficient.
- E-Commerce reduces paper work a lot.
- E-Commerce increased the productivity of the organization. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-in-time manufacturing way.

Advantages to Customers:

- 24x7 Support. Customer can do transactions for the product or enquiry about any product/services provided by a company any time, any where from any location. Here 24x7 refers to 24 hours of each seven days of a week.

- E-Commerce application provides user more options and quicker delivery of products.
- E-Commerce application provides user more options to compare and select the cheaper and better option.
- A customer can put review comments about a product and can see what others are buying or see the review comments of other customers before making a final buy.
- E-Commerce provides option of virtual auctions.
- Readily available information. A customer can see the relevant detailed information within seconds rather than waiting for days or weeks.
- E-Commerce increases competition among the organizations and as result organizations provides substantial discounts to customers.
- Advantages to Society
- Customers need not to travel to shop a product thus less traffic on road and low air pollution.
- E-Commerce helps reducing cost of products so less affluent people can also afford the products.
- E-Commerce has enabled access to services and products to rural areas as well which are otherwise not available to them.
- E-Commerce helps government to deliver public services like health care, education, social services at reduced cost and in improved way.

Disadvantages :-

E-Commerce disadvantages can be broadly classified in two major categories:

- Technical disadvantages
- Non-Technical disadvantages

Technical Disadvantages:

- There can be lack of system security, reliability or standards owing to poor implementation of e-Commerce.
- Software development industry is still evolving and keeps changing rapidly.

- In many countries, network bandwidth might cause an issue as there is insufficient telecommunication bandwidth available.
- Special types of web server or other software might be required by the vendor setting the e-commerce environment apart from network servers.
- Sometimes, it becomes difficult to integrate E-Commerce software or website with the existing application or databases.
- There could be software/hardware compatibility issue as some E-Commerce software may be incompatible with some operating system or any other component.

Non-Technical Disadvantages:

- Initial cost: The cost of creating / building E-Commerce application in-house may be very high. There could be delay in launching the E-Commerce application due to mistakes, lack of experience.
- User resistance: User may not trust the site being unknown faceless seller. Such mistrust makes it difficult to make user switch from physical stores to online/virtual stores.
- Security/ Privacy: Difficult to ensure security or privacy on online transactions.
- Lack of touch or feel of products during online shopping.
- E-Commerce applications are still evolving and changing rapidly.
- Internet access is still not cheaper and is inconvenient to use for many potential customers like one living in remote villages.

1.4 Benefits to Organization

1. Reduction of Cost per Contact:

In personal contacts, any sales Representative should pay full attention in one-to-one interaction. Lot of time, money and labor resources should be allocated for such one-on-one interaction.

A web based chat or e-mail involves a relatively low cost per contact. E-mail are generally handled in batches. The customer support executive while communicating with potential customers on the web can handle other functions between sessions during a live chat. It reduces cost incurred on labor which reduces the cost incurred on each contract. Using technology to acquire customers decreases the customer acquisition cost.

2. ***Creation of Intimate Relationship:***

Computer mediated chats create and support intimate relationship between refined method of' answering queries help to develop emotional bondage between the representative and the customer.

An integrated database to deliver consistent and improved customer responses improves the service level agreements and enhances the relationship between the customers and the business.

3. ***Reduction of Human Errors:***

"To err is Human". Errors may creep in when the customer support executive lacks training or influenced by moods. Computer-enabled communication results in less errors in relation to tracking orders, identifying the customer base and verifying the charges. If the data of the customers are accurately fed into the computer, then the reports generated on customers will be very accurate and meaningful to business organizations.

4. ***Quality of Work:***

The interaction between the customers and the representatives are generally monitored in business with computer mediated communications. Various business organizations also provide incentives to customer support executives based on their performances. This motivates and influences them to provide better and consistent service as they are subject to quality control and performance appraisal.

5. ***Good Return on Investment:***

Low cost per contact, outsourcing of customer support functions and filling up the customer representative post with temporary and seasonal workforce generate good return to any organization. An E-Commerce transaction reduces the cost on middlemen, advertisement and labor and generates good return on investment.

6. Generates Revenue:

Using interactive service tools to sell various products helps to decrease cost of product which in turn increases revenue and retail customers. Technology enabled business helps to shorten the sales cycle of the firm and increase sales performance such as revenue per sales representative and per Customer, average order size etc.

7. Quick Response:

The customer support executives respond to customer queries quickly. The services of the organization are available 24/7 x 365. Likewise, the supporting staff is well trained to handle queries. Such quick response brings satisfaction to customers and help business organization to retain customers.

8. Reduction of Development Time:

It is very expensive to train, motivate, influence and retain customer support executives. The image and the performance of the customer support executive have an impact on the image of the business organization. So, it is vital to recruit a pleasant looking customer support executive in traditional business.

1.5 Benefits to Society

The following are some of the advantages that e-commerce offers to the society.

1. Provides Job Opportunities:

E-commerce bridges the gap between the job seekers and job givers in the society. Human resources are able to get themselves placed in any organization by posting resumes through internet; some organizations also permit people to work from their home. E-commerce through internet provides a global wide network to identify and train human resource too.

2. Promotes Cordial Relationship:

E-commerce enables people to send gifts, greetings and gift vouchers to friends and relatives anywhere in the world. This promotes cordial relationship between and among individuals in the society.

3. ***Provides A Wealth of Information:***

   People through internet are able to access any information, say from tourism to financial products. Access of global information at lower cost, just by click of a button enhances the knowledge of the people and helps them to transform into a part of a knowledge-based society.

4. ***Provides Entertainment:***

   E-commerce helps people to download music, videos and go through latest updates and reviews. It permits people to book tickets to the movies online.

5. ***Less Pollution:***

   People can buy any product or service from any location through internet without traveling from their respective home or workplace. Business associates can contact each other from their locations. It reduces traffic and reduces air pollution and contributes to lessen global warming.

6. ***Online Education:***

   E-commerce enables the students' community to learn and acquire knowledge through online. Students can complete assignments and download information at anytime. Discussions with the tutors and with other students can take place with the help of internet.

   Students can enroll themselves in any online educational institution and acquire global exposure at a lower cost. Online education gives an opportunity for every student to participate in virtual classroom without considering their status, gender and role differences in the society.

7. ***Health Care:***

   Medical care and counseling are also provided through internet to the needed people. Doctors and nurses can get professional information and update themselves with the latest health care technologies through internet. This equips the doctors to provide good health care to their patients at a lower cost.

Benefits of E-Commerce to Nation

The following are some of the advantages that e-commerce offers to the Nation..

1. ***Reduces Regional Imbalances***

Developing countries provide several tax concessions for setting up call centers in remote and rural areas. Call centers provide a lot of employment opportunities. The revenues generated by the nation are allocated towards the development of infrastructure in the rural areas. It brings balanced regional development in the developing countries.

2. ***Reduces Unemployment***

Business organizations require talented human resources to develop and maintain the website of their business. Though business processes are automated, business organization require people to attend to customer queries. The establishment of call centers in developing countries reduces the unemployment problem of those countries.

3. ***Economic Development***

Business organizations are able to attract customers from anywhere in the world. Increase in customer base results in increased production. This generates greater revenues to the organizations and fosters expansion in national income. Expansion of national income and increase in the volume of production and services accelerate economic growth.

4. ***Availability of Goods***

Through internet people can buy goods from anywhere in the world. The goods which are not available locally can be purchased from any part of the world. The needs of the customers are met by accessing the internet. So, business organizations cannot ride on customers by citing shortage of goods in the local market as the reason.

1.6 Forces behind E Commerce Industry Framework

The evolution and growth of e-commerce can be attributed to a combination of technological, marketing and economic forces. Let us discuss some of the driving forces of e-commerce.

Economic Forces That Drives E-Commerce:

- E-commerce enables businesses to interact with suppliers, customers and with players in the distribution channel at a lower cost.

- The cost of installing and maintaining a website is much cheaper than owning a physical store. This motivates the growth of e-commerce.
- E-commerce generates greater profits due to less human intervention, lower overhead cost, few clerical errors and more efficiency.
- The cost of advertising is cheaper and provides access to global market at low cost. This is something which encourages people engaged in business to promote their business through electronic medium.
- Reduction in communication cost and technological infrastructure expense drive business towards e-business.
- Increase in competition and the rise in consumer power, 'globalization wave' have forced the business organizations to penetrate into internet world.

Technological Forces That Drives Electronic Commerce:

- Technological advances have made business communication faster, easier, economical and efficient. It has enabled the business to switch over from the local market to the global market.
- The growing popularity of cyber cafes has created a big role in attracting internet population towards e-commerce.
- Technological changes have given confidence to consumers to make electronic payments in settlement of financial obligations.

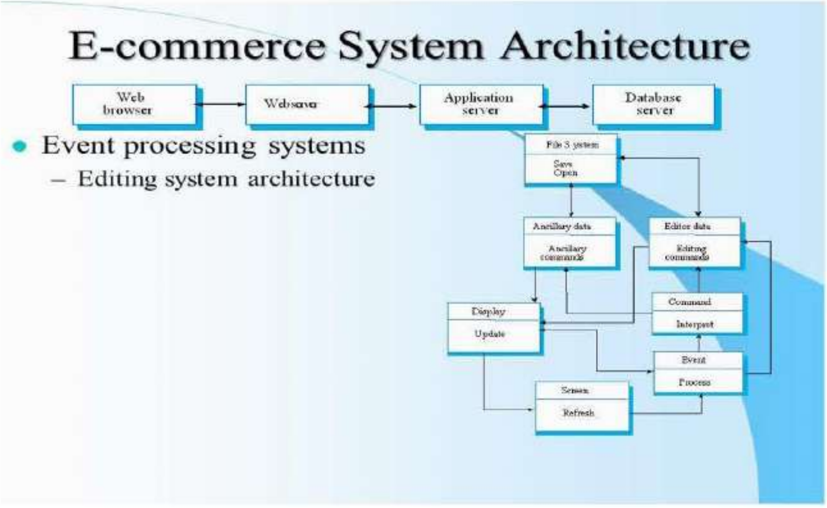
Market Forces That Drives Electronic Commerce:

- Business organizations are able to reach international markets by using electronic medium for enhanced customer support and service.
- E-commerce enables customers to make product comparison, place orders, track orders and make payments at ease. Due to convenience, customers prefer to purchase their desired goods or services over internet in the online marketplace.
- E-commerce also allows the customers to choose and order products according to their personal and unique specifications. It paves way for mass customization.
- The growing internet population stimulates business to switch over from an additional business to e-business.

- The great variety of commodities available online and reliable payment methods are regarded as contributors to the increase of e-business.
- Consumers often prefer shopping on the internet due to convenience and the changes in consumer behavior pulls consumer towards e-commerce.

1.7 Architectural Framework

The software framework necessary for building electronic commerce applications is little understood in existing literature. In general a framework is intended to define and create tools that integrate the information found in today's closed systems and allows the development of e-commerce applications. It is important to understand that the aim of the architectural frame-work itself is not to build new database management systems, data repository, computer languages, software agent based transaction monitors, or communication protocols Rather, the architecture should focus on synthesizing the diverse resources already in place in corporations to facilitate the integration of data and software for better applications.


E-commerce System Architecture

- Event processing systems
  - – Editing system architecture

Figure 1.1: E-Commerce System Architecture

The electronic commerce application architecture consists of six layers of functionality, or services:

- Applications;
- Brokerage services, data or transaction management;
- Interface, and; support layers"

- Secure messaging, security and electronic document Interchange;
- Middle ware and structured document interchange; and
- Network infrastructure and basic communications services

These layers cooperate to provide a seamless transition between today's computing resources and those of tomorrow by transparently integrating information access and exchange within the context of the chosen application. As seen in table above, electronic commerce applications are based on several elegant technologies. But only when they are integrated do they provide uniquely powerful solutions.

Application services	Customer- to- business Business- to- business Intra-organizational
Brokerage and data management	Order processing Payment advances-electronic cash Virtual mail
Interface layer	Interactive catalogues Directory support functions Software agents
Secure messaging	Encrypted e-mail, EDI Remote programming
Middle ware services	Structured documents (SCML,HTML) Compound documents
Network infrastructure	Wireless - cellular, radio, PCs Wire line – POTS, coaxial, fibre optic

1.8 Self Learning Exercise

Q.1 By Electronic Commerce we mean:

a) Commerce of electronic goods

b) Commerce which depends on electronics

c) Commerce which is based on the use of internet

d) Commerce which is based on transactions using computers connected by telecommunication network

Q.2 Disadvantages of e-Commerce in India are

(i) internet access is not universally available

(ii) Credit card payment security is not yet guaranteed

(iii) Transactions are de-personalized and human contact is missing

(iv) Cyberlaws are not in place

a) i and ii

b) ii and iii

c) i, ii, iii

d) i, ii, iii, iv

Q.3 A business competing in a commodity like environment must focus on which of the following?

a) Price

b) Ease / speed of delivery

c) Ease of ordering

d) all of the above

1.9 Summary

As the internet grew up and spread amongst all the countries of world, life of people were affected by this giant technology. Almost all aspects of their life style were somehow changed, and some online aspects were added. Nowadays, one of the most important subjects in online world is online jobs and internet home e-commerce. E-commerce means "buying and selling the products or services on internet or other networks". The use of commerce is conducted in this way.

1.10 Glossary

PPC – Pay per click : a form of advertising where you bid on specific keywords :nd pay every time someone clicks your advert (and is directed to your website). Google Adwords is the most well-known example of a PPC network.

Payment Gateway : the payment processor used to handle transactions on your ecommerce store, your payment gateway can be either on-site or off-site, depending on what works best for your model.

Paypal : one of the leading payment processors, preferred by a number consumers over any other single payment method. Owned by Ebay, Paypal is an essential component of your ecommerce payment setup.

Pay Per Click : a type of online advertising where you bid per click on highly targeted traffic, paying online for each click through to your website, rather than paying for impressions or some other metric.

SEO – Search engine optimization: the process of setting out your website and building links in a Google-friendly way, to ensure your website is given the best possible ranking within relevant SERPs.

1.11 Answers to Self-Learning Exercise

Q.1 (d)

Q.2 (c)

Q.3 (d)

1.12 Exercise

Q. 1 Which products are people most likely to be more uncomfortable buying on the Internet?

a) Books

b) Furniture

c) Movies

d) All of the above

Q.2 The solution for all business needs is

a) EDI

b) ERP

c) SCM

d) None of the above

Q.3 Which is a function of E-commerce

a) marketing

b) advertising

c) warehousing

d) all of the above

Q.4 What are materials used in production in a manufacturing company or are placed on the shelf for sale in a retail environment?

a) Direct materials

b) Indirect materials

c) EDI

d) None of the above

Q.5 What are plastic cards the size of a credit card that contains an embedded chip on which digital information can be stored?

a) Customer relationship management systems cards

b) E-government identity cards

c) FEDI cards

d) Smart cards

Q.6 Which of the following is a useful security mechanism when considering business strategy and IT?

a) encryption

b) decryption

c) firewall

d) all the above

1.13 Answers to Exercise

Q.1	(c)
Q.2	(b)
Q.3	(d)
Q.4	(a)
Q.5	(d)
Q.6	(d)

References and Suggested Readings

1. Third of internet users too scared to use credit card to shop online. (2009). Retrieved: May 12, 2009 from The Telegraph.

2. Harland, C.M. (1996) Supply Chain Management, Purchasing and Supply Management, Logistics, Vertical Integration, Materials Management and Supply Chain Dynamics. In: Slack, N (ed.) Blackwell Encyclopedic Dictionary of Operations Management. UK: Blackwell.

3. "Internet Marketing - How, When, Where?". Daily Mirror. http://print.dailymirror.lk/business/127-local/38977.html. Retrieved 24 March 2011.

4. Transaction Processing Performance Council website, available at: http://www.tpc.org/.

5. Kantor, Michael; James H. Burrows (1996-04-29). "Electronic Data Interchange (EDI)". National Institute of Standards and Technology. http://www.itl.nist.gov/fipspubs/fip161-2.htm. Retrieved 2008-05-13.

UNIT-2
Traditional Commerce v/s E-Commerce

Structure of the Unit

2.0 Objective

In this chapter we shall focus upon the following topics

- Traditional Business Model
- Electronic Business Model
- Comparison of both Business Models
- Technical and Non-Technical Aspects
- EDI

2.1 Traditional Business Commerce

Traditional commerce refers to the practice of selling products and services within a single industry and in some cases, within a specific geographical area. Traditional commerce relies on operating business hours during a specific period of time and requires housing inventory or occupying a retail store.

In contrast to e-commerce that relies on online sales, drop shipments and 24 hour access for consumers, traditional commerce relies more on local consumers interacting with sales executives, managers, customer service personnel and accountants personally versus through electronic mediums.

Businesses deemed as traditional commerce handle advertising, inventory shipping and creation of products and services in-house with a staff of employees in close proximity. Traditional commerce does not typically share information with competitors whereas e-commerce prices, specials and inventory are ready available online for consumers and competitors.

Traditional commerce often relies on face to face interaction with consumers and thrives based on word of mouth, networking and customer referrals for new and repeat business. Personal interaction is a key component of businesses experience success with traditional commerce. Many businesses network within the community, establish rapport with city leaders and chambers of commerce and sponsor local events and sports teams to develop a relationship with the community to draw in business.

2.2 Rules for Traditional Commerce

- The traditional Commerce is based on the following rules. It needs to hire sales executive, sales managers, accountants, and other staffs.
- Operates at business hours within a certain period of time.
- Requires location renting/purchasing, staff employment, advertising, inventoryshipping and handling all sums up the high-cost equation which makes many people negate from starting a business entirely.
- No sharing of the information with the competitors.
- The basis of a traditional business depends on the frequency of new and oldcustomers buying from them to keep the business running.

2.3 Difference between E-Commerce and Traditional Commerce

Figure 2.1: Difference between E-Commerce and Traditional Commerce

1. ***Cost Effective:***

E-commerce is very cost effective when compared to traditional commerce. In traditional commerce, cost has to be incurred for the role of middlemen to sell the company's product. The cost incurred on middlemen is eliminated in e-commerce as there is a direct link between the business and the customer. The total overhead cost required to run e-business is comparatively less, compared to traditional business.

For example, in running an e-business, only a head office is required. Whereas in traditional method, a head office with several branches are required to cater to the needs of customers situated in different places. The cost incurred on labour, maintenance, office rent can be substituted by hosting a website in e-business method.

2. ***Time Saving:***

It takes a lot of time to complete a transaction in traditional commerce. E-commerce saves a lot of valuable time for both the consumers and business. A product can be ordered and the transaction can be completed in few minutes through internet.

3. ***Convenience:***

E-commerce provides convenience to both the customers and the business. Customers can browse through a whole directories of catalogues, compare prices between products and choose a desired product any time and anywhere in the world without any necessity to move away from their home or work place.

E-commerce provides better connectivity for its prospective and potential customers as the organization's website can be accessed virtually from anywhere, any time through internet. It is not necessary to move away from their work place or home to locate and purchase a desired product.

4. ***Geographical Accessibility:***

In traditional commerce, it may be easy to expand the size of the market from regional to national level. Business organizations have to incur a lot of expenses on investment to enter international market. In e-commerce it is easy to expand the size of the market from regional to international level.

By hosting a website, by placing advertisements on the internet and satisfying certain legal norms, a business can penetrate into global market. It is quite easy to attract customers from global markets at a marginal cost.

5. ***Introduction of New Products:***

In traditional commerce, it takes a lot of time and money to introduce a new product and analyze the response of the customers. Initially, cost has to be incurred to carry out pilot surveys to understand the taste of the customers.

In e-commerce, it is easy to introduce a product on the website and get the immediate feedback of the customers. Based on the response, the products can be redefined and modified for a successful launch.

6. ***Profit:***

E-commerce helps to increase the sales of the organization. It helps the organization to enjoy greater profits by increasing sales, cutting cost and streamlining operating processes.

The cost incurred on the middlemen, overhead, inventory and limited sales pulls down the profit of the organization in traditional commerce.

7. ***Physical Inspection:***

E-commerce does not allow physical inspection of goods. In purchasing goods in e-commerce, customers have to rely on electronic images whereas in traditional commerce, it is possible to physically inspect the goods before the purchase.

8. ***Time Accessibility:***

Business is open only for a limited time in traditional commerce. Round the clock (24 x 7) service is available in e-commerce.

9. Product Suitability:

E-commerce is not suitable for perishable goods and high valuable items such as jewellery and antiques. It is mostly suitable for purchasing tickets, books, music and software. Traditional commerce is suitable for perishables and touch and feel items. Purchasing software, music in traditional commerce may appear expensive,

10. Human Resource:

To operate in electronic environment, an organization requires technically qualified staff with an aptitude to update themselves in the ever changing world. E-business has difficulty in recruiting and retaining talented people. Traditional commerce does not have such problems associated with human resource in non electronic environment.

11. Customer Interaction:

In traditional commerce, the interaction between the business and the consumer is a "face-to-face".

In electronic commerce, the interaction between the business and the consumer is "screen-to-face". Since there is no personal touch in e-business, companies need to have intimate relationship with customers to win over their loyalty.

12. Process:

There is an automated processing of business transactions in electronic commerce. It helps to minimize the clerical errors.

There is manual processing of business transactions in traditional commerce. There are chances of clerical errors to occur as human intervention takes place.

13. Business Relationship:

The business relationship in traditional commerce is vertical or linear, whereas in electronic commerce the business relationship is characterized by end-to-end.

14. Fraud:

Lots of cyber fraud takes place in electronic commerce transactions. People generally fear to give credit card information. Lack of physical presence in markets and unclear legal issues give loopholes for frauds to take place in e-business transactions.

Fraud in traditional commerce is comparatively less as there is personal interaction between the buyer and the seller.

Sr. No.	Traditional Commerce	E-Commerce
1	Heavy dependency on information exchange from person to person.	Information sharing is made easy via electronic communication channels making little dependency on person to person information exchange.
2	Communication/ transaction are done in synchronous way. Manual intervention is required for each communication or transaction.	Communication or transaction can be done in asynchronous way. Electronics system automatically handles when to pass communication to required person or do the transactions.
3	It is difficult to establish and maintain standard practices in traditional commerce.	A uniform strategy can be easily established and maintain in e-commerce.
4	Communications of business depends upon individual skills.	In e-Commerce or Electronic Market, there is no human intervention.
5	Unavailability of a uniform platform as traditional commerce depends heavily on	E-Commerce website provides user a platform where al l information is available at one place.

	personal communication.	
6	No uniform platform for information sharing as it depends heavily on personal communication.	E-Commerce provides a universal platform to support commercial / business activities across the globe.

Table 2.1

2.4 Technical & Nontechnical Limitations Commerce

Though e-commerce offers many advantages to customers, business, society and nation, there are still some areas of concern that need to be addressed. The following are some of the limitations or disadvantages of e-commerce.

1. Security:

The biggest drawback of e-commerce is the issue of security. People fear to provide personal and financial information, even though several improvements have been made in relation to data encryption. Certain websites do not have capabilities to conduct authentic transactions. Fear of providing credit card information and risk of identity limit the growth of e-commerce.

2. Lack of Privacy:

Many websites do not have high encryption for secure online transaction or to protect online identity. Some websites illegally collect statistics on consumers without their permission. Lack of privacy discourages people to use internet for conducting commercial transactions,

3. Tax Issue:

Sales tax is another bigger issue when the buyer and seller are situated in different locations. Computation of sales tax poses problems when the buyer and seller are in different states. Another factor is that physical stores will lose business if web purchases are free from tax.

4. Fear:

People fear to operate in a paperless and faceless electronic world. Some of the business organizations do not have physical existence, People do not know with whom they are conducting commercial transactions. This aspect makes people to opt physical stores for purchases.

5. ***Product Suitability:***

   People have to rely on electronic images to purchase products. Sometimes, when the products are delivered, the product may not match with electronic images. Finally, it may not suit the needs of the buyers. The lack of 'touch and feel' prevent people from online shopping.

6. ***Cultural Obstacles:***

   E-commerce attracts customers from all over the world. Habits and culture of the people differ from nation to nation. They also pose linguistic problems. Thus, differences in culture create obstacles to both the business and the consumers.

7. ***High Labour Cost:***

   Highly talented and technically qualified workforce are required to develop and manage the websites of the organization. Since internet provides a lot of job opportunities, business organizations have to incur a lot of expenses to retain a talented pool of employees,

8. ***Legal Issues:***

   The cyber laws that govern the e-commerce transactions are not very clear and vary from country to country. These legal issues prevent people from entering into electronic contracts.

9. ***Technical limitations:***

   Some protocol is not standardized around the world. Certain software used by

   vendor to show electronic images may not be a common one. It may not be possible to browse through a particular page due to lack of standardized software. Insufficient telecommunication bandwidth may also pose technical problems.

10. ***Huge Technological Cost:***

    It is difficult to merge electronic business with traditional business. Technological infrastructure may be expensive and huge cost has to be incurred to keep pace with ever changing technology. It is necessary to allocate more funds for technological advancement to remain competitive in the electronic world.

2.5 Enterprise Data Interchange (EDI)

EDI, which has been used for some 20 years, describes the electronic exchange of standard business documents between firms. A structured, standardized data format is used to exchange common business documents (e.g., invoices and shipping orders) between trading partners. In contrast to the free form of e-mail messages, EDI supports the exchange of repetitive, routine business transactions. Standards mean that routine electronic transactions can be concise and precise. The main standard used in the U.S. and Canada is known as ANSI X.12, and the major international standard is EDIFACT. Firms following the same standard can electronically share data. Before EDI, many standard messages between partners were generated by computer, printed, and mailed to the other party that then manually entered the data into its computer.

The main advantages of EDI are:

- Paper handling is reduced, saving time and money;
- Data are exchanged in real time;
- There are fewer errors since data are keyed only once;
- Enhanced data sharing enables greater coordination of activities between business partners;
- Money flows are accelerated and payments received sooner.

Despite these advantages, for most companies EDI is still the exception, not the rule. A recent survey in the United States showed that almost 80 percent of the information flow between firms is on paper. Paper should be the exception, not the rule. Most EDI traffic has been handled by value-added networks (VANs) or private networks. VANs add communication services to those provided by common carriers (e.g., AT&T in the U.S. and Telstra in Australia). However, these networks are too expensive for all but the largest 100,000 of the 6 million businesses in existence today in the United States.

As a result, many businesses have not been able to participate in the benefits associated with EDI. However, the Internet will enable these smaller companies to take advantage of EDI. Internet communication costs are typically less than with traditional EDI. In addition, the Internet is a global network potentially accessible by nearly every firm. Consequently, the Internet is displacing VANs as the electronic transport path between trading partners. The simplest approach is to use the Internet as a means of replacing a VAN by using a commercially available Internet EDI package. EDI, with its roots in the 1960s, is a system for exchanging text, and the opportunity to use the multimedia capabilities of the Web is missed if a pure replacement strategy is applied. The multimedia capability of the Internet creates an opportunity for new applications that spawn a qualitatively different type of information exchange within a partnership. Once multimedia capability is added to the information exchange equation, then a new class of applications can be developed (e.g., educating the other partner about a firm's purchasing procedures).

2.6 Self Learning Exercise

Q.1 B2C commerce

a) includes services such as legal advice

b) means only shopping for physical goods

c) means only customers should approach customers to sell

d) means only customers should approach business to buy

Q.2 Electronic Data Interchange is necessary in

a) B2C e-Commerce

b) C2C e-Commerce

c) B2B e-Commerce

d) Commerce using internet

Q.3 EDI requires

a) representation of common business documents in computer readable forms

b) data entry operators by receivers

c) special value added networks

d) special hardware at co-operating Business premises

E-commerce is a new way of conducting, managing and executing business transactions using computer and telecommunications networks. As awareness of the Internet throughout the commercial world and general public increases, competitiveness will force lower entry barriers, continued rapid innovation and expansion of markets. The real key to making electronic commerce over the Internet a normal, everyday business activity is the convergence of the telecommunications, content/media and software industries. E-Commerce is expected to improve the productivity and competitiveness of participating businesses by unprecedented access to an on-line global market place with millions of customers and thousands of products and services.

2.8 Glossary

EDI: Electronic Data Interchange.

CGI Script: Common gateway Interface is a scripting system designed to work with HTTP Web Servers. The scripts, usually written in the Perl coding language, are ofter used to exchange data between a Web server and databases.

Digital Cash: An electronic replacement of cash.

Joint Electronic Payments Initiative (JEPI): This initiative, led by the World Wide Web Consortium and CommerceNet, is an attempt to standardize payment negotiations. On the buyer's side (the client side), JEPI serves as an interface that enables a Web browser, and wallets, to use a variety of payment protocols. On the merchant's side(the server side), JEPI acts between the network and transport layers to pass off the incoming transactions to the proper transport and payment protocols.

Microcash: Small denomination digital tokens.

Microtransactions: Low-cost, real-time transactions using microcash.

Smart Cards: A credit card-sized plastic card with a special type of integrated circuit embedded in it. The integrated circuit holds information in electronic form and controls who uses this information and how.

Tokens: Strings of digits representing a certain amount of currency. The issuing bank validates each token with a digital stamp.

Value Added Networks: Networks that are maintained privately and dedicated to EDI between business parteners.

2.9 Answers to Self-Learning Exercise

Q.1 (a)

Q.2 (c)

Q.3 (a)

2.10 Exercise

Q.1 Advantages of B2C commerce to customers are

(i) wide variety of goods can be accessed and comparative prices can be found

(ii) shopping can be done at any time

(iii) privacy of transactions can be guaranteed

(iv) security of transactions can be guaranteed

a) i and ii

b) ii and iii

c) iii and iv

d) i and iv

Q.2 EDI standards are

a) not universally available

b) essential for B2B commerce

c) not required for B2B commerce

d) still being evolved

Q.3 In B2B e-Commerce

(i) Co-operating Business should give an EDI standard to be used

(ii) Programs must be developed to translate EDI forms to a form accepted by application program

(iii) Method of transmitting/receiving data should be mutually agreed

(iv) It is essential to use internet

a) i, ii

b) i, ii, iii

c) i, ii, iii, iv

d) ii, iii, iv

Q.4 By security in e-Commerce we mean

(i) Protecting an organization's data resource from unauthorized access

(ii) Preventing disasters from happening

(iii) Authenticating messages received by an organization

(iv) Protecting messages sent on the internet from being read and understood by unauthorized persons/organizations

a) i, ii

b) ii, iii

c) iii, iv

d) i, iii, iv

Q.5 What is the process in which a buyer posts its interest in buying a certain quantity of items, and sellers compete for the business by submitting successively lower bids until there is only one seller left?

a) B2B marketplace

b) Intranet

c) Reverse auction

d) Internet

Q.6 Most individuals are familiar with which form of e-commerce?

a) B2B

b) B2C

c) C2B

d) C2C

Q.7 Which form of e-commerce currently accounts for about 97% of all e-commerce revenues?

a) B2B

b) B2C

c) C2B

d) C2C

Answers:-

Q. 1 (a)

Q. 2 (b)

Q. 3 (b)

Q. 4 (d)

Q. 5 (c)

Q. 6 (b)

Q. 7 (a)

References and Suggested Readings

1. Internet Commerce: Digital Models for Business, Lawrence et al, Wiley
2. Electronic Commerce: A Manager's Guide, Kalakota et al, Addison-Wesley
3. Web Commerce Technology Handbook, Minoli et al, McGraw Hill
4. The Economics of Electronic Commerce, Choi et al, MacMillan
5. Designing Systems for Electronic Commerce, Treese et al, Addison-Wesley
6. Laudon, Kenneth C.; Guercio Traver, Carol (2014). E-commerce. business. technology. society. 10th edition. Pearson. ISBN 978-013-302444-9.
7. Chaudhury, Abijit; Kuilboer, Jean-Pierre (2002). e-Business and e-Commerce Infrastructure. McGraw-Hill. ISBN 0-07-247875-6.

UNIT-3
E- Commerce Models

Structure of the Unit

3.0 Objective

- Recognize the key segments of E-Commerce plans of action.
- Describe the major B2C plans of action.
- Describe the major B2B plans of action.
- Describe plans of action in other rising ranges of E-Commerce.
- Explain the key business ideas and techniques relevant to E-Commerce

3.1 Introduction

At the point when an organization is establish it E-Commerce technique, that is, from the definition, no existing information by which construct a E-commerce model. As a rule, that is simply not a considerable measures of information accessible on how E-Commerce is getting along — and surely not as far as benefit since the information is constantly collapsed into some bigger number (with the exception of the odd traded on an open market unadulterated player). there is not a considerable measure of ability with past experience to go. The principle examination in set up an E- Business site must concentrate on three point:

- set up correct fit with trade name image
- adjust to the company traditions
- think about the fit/blend with the active channels.

3.2 Business -to -Business Model (B2B)

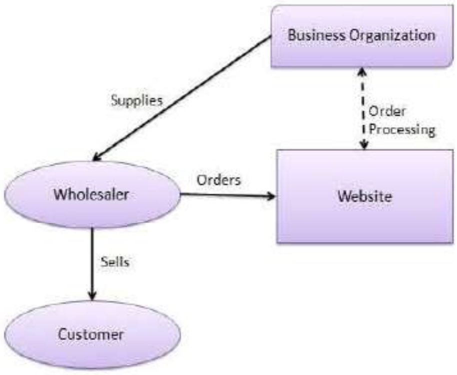
Website accepting after B2B model plan of action provide it item to a man that purchase the item and then offer item to end client. For at a moment, a seller puts a request from organization site and in wake of accepting the committal, offers the finished result to conclusive customer who come to procure the item at on a big scale to distribute in market. B2B infers that vender and in addition customer is business part. B2B model cover huge number of utilizations which empower business to shape associations with their merchant, supplier . The main important thing in B2B Model is:

- Electronic item
- Warehousing
- Shipping
- Vehicles
- Petrochemicals
- Office products
- Food
- Agriculture
- Paper

Following are the key technologies used in B2B e-commerce :-

- **Electronic Data Interchange (EDI)** – It is a bury authoritative trade of business archives in an organized and machine process able configuration.

- **Internet** – Internet speaks to internet or system of systems associating PCs over the world.
- **Intranet** – Intranet speaks to a committed system of PCs inside a one association .
- **Extranet** – It speaks to a system where outer business accomplices, supplier or clients can have constrained access to a partition of big business intranet/arrange.
- **Back-End Information Systems Integration** – Back End data frameworks are database administration frameworks used to deal with business information.



Architectural models in B2B e-commerce –

- **Supplier Orient marketplace** –this type of model include, a typical commercial centre gave by supplier is utilized by both individual clients and in addition business clients. the supplier provide electronic-stores for deals advancement.
- **Purchaser Orient marketplace** –this type of model include, purchaser has personal particular commercial centre or electronic-advertise. He welcomes suppliers to offer on item's index. A Buyer organization opens an offering site.
- **Middle person Orient marketplace** – this type of model include, a mediator organization maintains a commercial centre where business purchasers and merchants can execute with each other.
- **Online marketplace-** Online marketplace is not like straight-up E-retail outlet. In straight-up E-retail a company sell all items on the net and in

online marketplaces many third party can set up stalls and use it for selling to customers. Online marketplace come in B2B model and C2C model.

- **Catalogue sites -**This term is use to depict B2B E-commerce site in which we can browse through retailer stock via category and put the order using website. There are a large range of catalogue sites, covering each sector and industry.

3.3 Business to Consumer (B2C)

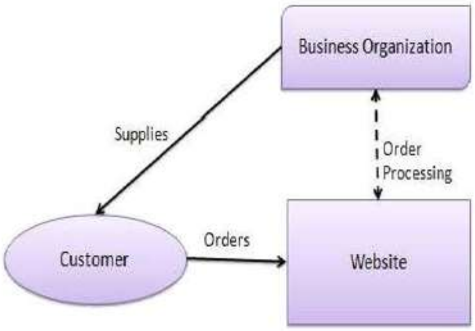
In Business to consumer Model, a buyer go to the site, chooses a catalogue, request the catalogue and a mail is sent to organization. After get the order , item send to the costumer.

Key elements of a B2C Model :

- Heavy advertisement requirement
- A very big investment require in Hardware/Software
- Customer support service of good and fast response.
- High interest as far as equipment/programming.
- Support or great client mind benefit.

Customer Shopping Procedure

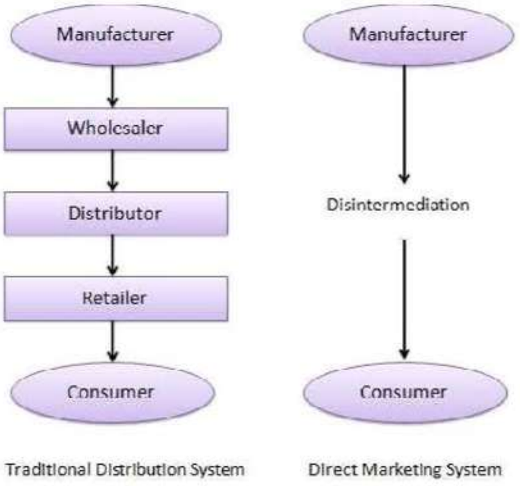
1. A purchaser
2. Identify the requirements
3. Find existing items on the website meet the requirements
4. Compare same type of items.
5. Put the order
6. Pay the bill
7. Receive the item and review the item.
8. Consult with vendor regarding service support .

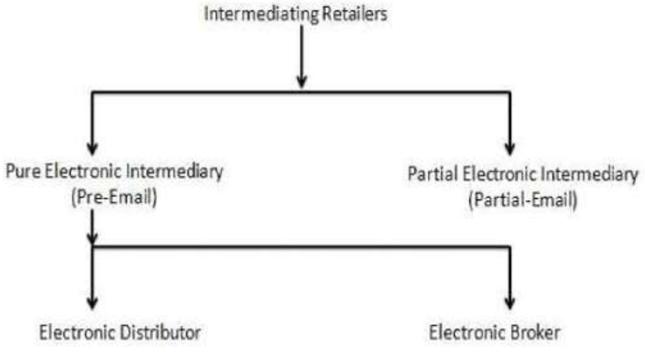


Disintermediation and Reinter Mediation:

In conventional business, there are intermediating operators like wholesalers, merchants, retailers amongst maker and purchaser. In B2C site, producer can offer items specifically to purchasers. This procedure of expulsion of business layers in charge of delegate capacities is called Disintermediation.

Presently another electronic middle person breed is developing like e-shopping centre and item choice specialists are rising. This procedure of moving of business layers in charge of middle person capacities from customary to electronic mediums is called Reinter intervention.




Intermediating Retailers
Pure Electronic Intermediary (Pre-Email)
Partial Electronic Intermediary (Partial-Email)
Electronic Distributor
Electronic Broker

Standard/Direct Retail

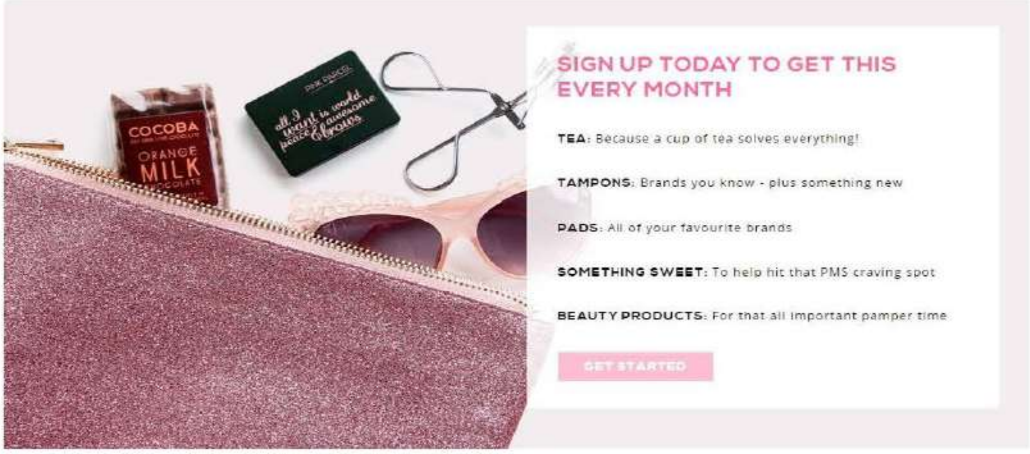
Above all else, obviously, we have the most "customary" and clear B2C ecommerce demonstrate: standard retail. The seller, a business, offers a thing (or more than one thing) to the purchaser, a buyer, who pays for it and afterward gets it. You could call this the default B2C ecommerce display, however it's in no way, shape or form the stand out – and can without much of a stretch be joined with different models for a more changed administration.

Subscription Ecommerce

Membership based administrations, regularly on the whole called the 'membership economy', have seen a colossal ascent in fame as of late over all businesses, including – or maybe particularly – ecommerce. They frequently appear as membership boxes, which are general conveyances of boxes containing products by the dealer.

A few sorts of membership box will convey a choice of new, irregular things – these are known as 'revelation boxes' – while different boxes will give particular, pre-decided things, called 'accommodation boxes'.

The membership model is utilized crosswise over ecommerce organizations of each assortment, from nourishment to distributed to hygiene. Graze, which offers solid snacks in thin cardboard membership boxes, has made extraordinary progress with this model starting in 2008. Other nourishment organizations, for example, Hello Fresh and Plated, offer membership boxes containing 'supper packs': every one of the fixings expected to make a sound dinner, intended to make solid cooking speedier and more helpful.



SIGN UP TODAY TO GET THIS EVERY MONTH

TEA: Because a cup of tea solves everything!

TAMPONS: Brands you know - plus something new

PADS: All of your favourite brands

SOMETHING SWEET: To help hit that PMS craving spot

BEAUTY PRODUCTS: For that all important pamper time

In the distributed business, memberships to daily papers and magazines are clearly exceptionally basic, yet one business has utilized this model to accomplish something somewhat distinctive: Stack is an organization which conveys an alternate autonomous magazine to its supporters consistently. Like the 'disclosure box' display, this framework permits endorsers of bolster the more extensive free magazine industry while finding new distributions all the time.

Other various organizations taking into account the membership fever incorporate the Close Shave Society, which conveys customary conveyances of men's extremely sharp edges; Pink Parcel, which conveys month to month bundles of sterile towels and look after 'that time'; and Ink Drops, a stationery membership benefit for significant others of transcribed letter-composing.

Social Shopping

Social shopping is a more up to date, yet at the same time best in class slant in ecommerce. There is a scope of various models inside the more extensive class of social shopping, including "purchase" catches on informal communities like Pinterest, Facebook and Twitter; shoppable recordings and exhibitions; and outsider social shopping locales.

Parts of social shopping can without much of a stretch be coordinated close by one of the other ecommerce models point by point in this article. Imprints and Spencer, for instance, is a B2C coordinate retail outlet which has incorporated shoppable video into its substance promoting.

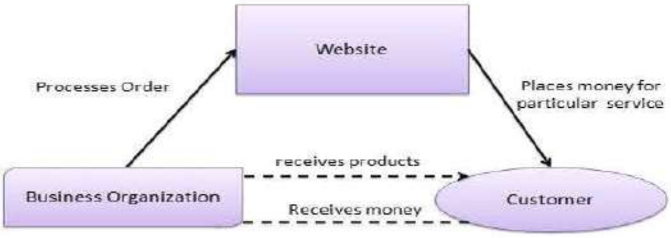
Credit Model

The purchaser credit model is one which is boundless in terrain Europe, however has just as of late advanced toward the UK and the US through ecommerce. Basically, it's a 'purchase now, pay later' framework which permits customers to buy things using a loan and be charged for them at a later date. Similarly as with Visas, there is normally intrigue charged on the credit, and clients can select to pay off the adjust after some time.

Example: Buy.com, Wal-Mart.com, BestBuy.com

3.4 Consumer to Business (C2B)

The fundamental standard of most C2B ecommerce, which separates it from normal B2C ecommerce, is that the shoppers are the ones making esteem for the items.



This should be possible through a turnaround sale or Name Your Own Price demonstrate, in which purchasers name the sum they will pay for an item, for example, travel tickets, and the exchange happens if the vender acknowledges the cost. (At the end of the day, it resembles internet wheeling and dealing).

An eminent case of this ecommerce model is Priceline.com, which offers ease travel items like flight tickets, auto rental and convenience to cost cognizant purchasers. Buyers get the advantage of purchasing administrations at decreased costs, while organizations can auction unused seats, rooms, and so on without publicizing the low cost to the overall population – the offering business' character is just uncovered after an exchange has effectively finished, and exchanges are additionally non-refundable.

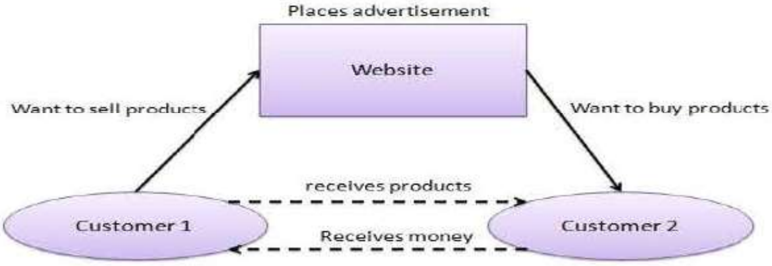
Another case of a C2B ecommerce display in which buyers make esteem for an item is the retailer Gilt, which was initially presented and took off in 2007, pretty much as the worldwide retreat and credit crunch was hitting organizations around the world.

Overlaid's plan of action includes offering overabundance stock from architect brands at steeply reduced costs to a very drew in group of individuals. It makes purchaser request around the merchandise, and permits design brands to exchange abundance stock without bargaining their top of the line picture or lose as much income as they generally may by auctioning to off-value retailers.

The C2B plan of action along these lines has a tendency to include making esteem around an item that may not generally be useful to organizations, and offering it at an advantage to both the purchaser and the dealer. There are additionally a modest bunch of ecommerce locales which are C2B in the more clear feeling of "shoppers offering to organizations, for example, Upwork, a stage for independent experts and contractual workers to publicize their administrations for contract by organizations.

3.5 Consumer to Consumer (C2C)

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



Online Marketplaces

Much as with B2B commercial centres, C2C online commercial centres are locales where shoppers can set up their own shops keeping in mind the end goal to offer products to different purchasers. The commercial centre will ordinarily benefit by charging a posting expense, and/or taking a cut of the last deal esteem when a thing is sold.

A deal on an online commercial centre can appear as a closeout, where imminent purchasers can offer expanding sums so as to win a thing, as eBay is best-known for; or it can appear as an immediate deal.

All through a large portion of the world, merchants who need to rundown things on a C2C commercial centre will normally look to either eBay or Amazon Marketplace, both of which are massively prominent and settled online commercial centres. In China, in any case, the undisputed market pioneer in C2C ecommerce is Taobao Marketplace, claimed by Alibaba Group.

Various littler C2C online commercial centres take into account more specialty dealers and groups of onlookers, for example, those which permit craftsmen and create devotees to offer their work to others. Etsy, a C2C commercial centre which works in handcrafted artworks and vintage products, is a standout amongst the most famous, with 54 million enrolled clients as of December 2014.

Society6 and Red bubble are two different cases of C2C commercial centres for free craftsmen, which permit specialists to offer their outlines on a scope of things including pads, encircled prints, cell phone cases, T-shirts and that's only the tip of the iceberg.

Crowd Funding

It may appear like pushing the meaning of "ecommerce" a bit to incorporate crowd funding, however I had an inclination that it merited a gesture here. Crowd funding sites like Kickstarter and Indiegogo frequently observe ventures propelled as a method for trialing or testing interest for an item that later goes ahead to be sold monetarily.

While the vast majority presumably don't go looking for items on crowd funding sites, they can even now be an extraordinary approach to buy something new and intriguing – a prepackaged game, say, or a biodegradable umbrella– the length of

you wouldn't fret the hold up and the hazard that accompanies backing a crowd funding venture.

A year ago Indiegogo recognized this with the dispatch of In Demand, an administration that encourages the move from crowd funding task to retail item, empowering effort proprietors to "consistently move into the following period of operations, including tolerating item pre-orders, client procurement and profit development."

Kickstarter has additionally assembled present aides on its blog of items that were initially crowd funded on its website and are as of now sold internet, urging clients to purchase a Kickstarter-subsidized thing as an uncommon Christmas present.

Numerous crowdfunding activities are utilized as a method for offering an item in a set number to a select gathering of people, for example, when a webcomic maker with a built up taking after needs to offer a constrained print keep running of their comic to their per users.

Thusly, crowd funding as often as possible goes about as an antecedent to or even a remain in for conventional ecommerce, making it definitely justified even despite a say on this rundown.

'Rental Ecommerce' – The Gig and Sharing Economy

The 21st century has seen the enormous take-off of both the gig and the sharing economy, or what I am likely naming 'rental ecommerce'. While regularly treated and ordered independently, the gig economy and sharing economy have a considerable measure of covers, and administrations which straddle the separation between the two.

Both at last spin around similar guideline of paying for a transitory administration, whether it's an auto to take you from A to B, a man to amass your level pack furniture, or a space to stay in for the night. The simplicity of digitally interfacing individuals who have things with individuals who require them has prompted an abundance of rental and accommodation administrations where practically anything can be gained incidentally.

Amazon's Mechanical Turk program is one of the most established cases of the digitally-empowered gig economy, and has been interfacing specialists for-contract with people and organizations that require their administrations since 2005. Amazon has since extended its stake in rental ecommerce with Amazon Flex, which employs brief drivers to convey Amazon allocates certain US urban communities.

Uber and AirBnB are two as often as possible referred to cases of industry disruptors from the universe of rental ecommerce, however incalculable other littler administrations have sprung up around there, began by standard people to take into account a particular corner. For instance, there are different sites equipped around interfacing pet proprietors with creature adoring pet sitters who will give mind administrations: Cat in a Flat, Borrow My Doggy, Pawshake to give some examples.

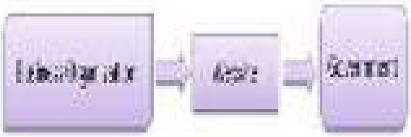
Rental ecommerce permits customers to lease anything from a parking spot to donning hardware to other people who require it, permitting them to monetise products that would somehow go to squander. It's purchasing and offering of an alternate kind than we've generally expected from ecommerce, yet is still both well known and beneficial.

3.6 Business - to - Government (B2G)

Business-to-government (B2G) is a subsidiary of B2B promoting and regularly alluded to as a market meaning of "open division showcasing" which envelops showcasing items and administrations to different government levels - including elected, state and neighbourhood - through coordinated advertising interchanges procedures, for example, key advertising, marking, marcom, publicizing, and electronic correspondences.

B2G systems give a stage to organizations to offer on government openings which are introduced as requesting as RFPs in an invert sell off form. Open part associations (PSOs) post tenders as RFPs, RFIs, RFQs, Sources Sought, and so on and suppliers react to them.

B2G E-Commerce



Government organizations commonly have pre-arranged standing contracts checking the sellers/suppliers and their items and administrations at set costs. These can be state, nearby or government contracts and some might be grandfathered in by different substances (i.e. California's MAS Multiple Award Schedule will perceive the national government get holder's costs on a General Services Administration Schedule).

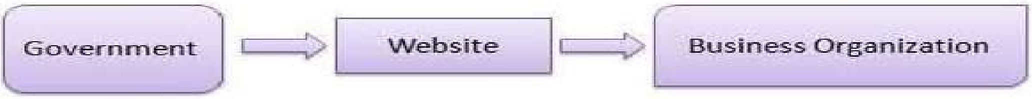
There are various social stages devoted to this vertical market and they have ascended in ubiquity with the onset of the ARRA/Stimulus Program and expanded government stores accessible to business elements for both allows and contracts

Business-to-government E-commerce can be defined as export and import between companies and the public region. It means use of the Internet for public procurement, licensing methods and other government-related business. This kind of E-commerce has two features first one is that the public supposed a leading role in establishment of E-commerce and second, it is unspecified that the public region has the maximum need for making its procurement system more successful. Web-based purchasing terms or policies reduce the hazard of irregularities and increase the precision of the procurement development. Today government e-procurement systems remain immature or we can say that it is not fully developed.

3.7 Government - to - Business (G2B)

G2B Model is part of electronic-administration. Using G2B Model the whole data and administrations are provide by Government to Business Organizations via unfathomable scheme of government sites.

Business Organization can receive data regarding business principles, requirement and authentication required for start other business, and different details.



A Business Organization can likewise download distinctive structures and submit it on the web or disconnected to the concern office.
example : http://www.incometaxindia.gov.in

G2B (Government to Business) is a term that alludes to the connections between associations (subjects) of open organization and undertakings (organizations). The assignment can be utilized for any relationship between the subject of open organization and the undertaking, frequently it is utilized as one of the fundamental relationship inside e-Government models. The activity originates from a government association (open organization) and undertakings are the objective gathering.

Utilization of the G2B by and by: G2B idea is utilized for communicating the relationship between open organization and undertakings. The relationship may allude the interest for data from the endeavours in any life circumstance or an exchange of an official report to the statutory body. The shortened form is generally used to allude to the ICT arrangement that proselytes such correspondence to the electronic shape or to portray an answer that improves the correspondence between open organization and ventures (e.g. web gateway of the obtainment power or electronic answers for buying).

3.8 Government-to-Citizen (G2C)

G2C Model is additionally use for electronic-administration.

The aim of the model is provide good and compelling administrations to each and every national.

Government
Website
Citizen

The Government provide the many information though website.

- Each and every administration office information,
- Many types of plan of welfare ,
- Many type of application format(structure) that is use by nationals.

The Gujarat Government has built up his own system called Gujarat State Wide Area Network (GSWAN) for similar reason said above.

example of this model is GSWAN.

http://gswan.gov.in

3.9 Intra and Inter Organization E- Commerce

Inter-Organizational Transaction

Business to business transactions covers a variety of situations. They vary from the regular repeat transactions. These transactions conform to differing trade cycles and are applicable to different

e-Commerce solutions:

- ➢ Electronic market
- ➢ Electronic data interchange
- ➢ Inter-organizational e-Commerce

Inter-Organizational Transactions:

Business organizations are constantly buying and selling goods and services. Shop buy product in bulk from their suppliers and selling goods in small quantities to their customers. Manufactures buy raw materials or components from their suppliers, assemble them into new products and sell them, in turn to their customers.

Electronic Commerce: Intra Organization

- Intranets are corporate networks that utilize the Internet technology but limit access to the internal members of an organization.
- Typically, they are built by securing it from the global Internet through a firewall that limits access to internal/authorized members only.
- Internal computer network that supports Internet applications qualifies to be called an Intranet.
- Typically, Intranets use TCP/IP connectivity and a HTTP server (Web server).
- Through Standard web browser users can tap into corporate legacydata, share applications and public

Electronic Commerce: Intra Organization

Intranet Offers following advantages

- Platform Independent and Portable Access
- Increase the reach of internal users through a portable, platform.
- Regardless of the type of platform the up-to date information can accessed from a common interface often based on Web browser.

Business to Employee (B2E) services

–Used for implementing improved Employee Relationship Management initiatives. B2E applications offer employees self-service capability on much of the human resource functions.

Intra Organization Integration

–the web can integrate the legacy systems spread across the organization. This expands the information available for decision-makers

3.10 Self Learning Exercise

Q.1 E- commerce for

a) electron commerce

b) electric commerce

c) electronic commerce

d) for all

Q.2 GSWAN is for

a) Gujrat state wide area network

b) Govt. state wide area network

c) Genral state wide area network

d) none

Q.3 In E-Commerce C2C Model is

a) Computer to Computer

b) Consumer to consumer

c) consumer to computer

d) none

Q.4 In E-Commerce B2C Model is

a) Business to Computer Model

b) Business to Contract Model

c) Business to Consumer Model

d) none

3.11 Summary

The basic development in Internet based business in a brief timeframe has underscored the requirement for comprehension the instruments and guessing the business models received by fruitful associations. We have started this procedure by giving a system to see how plans of action are intended for associations involving the Internet economy. The procedure has one been of making certain experimental speculations. Be that as it may, it takes into consideration hypothesis working in a few ways. For case, it is conceivable to build up a few suggestions and develops utilizing this structure for further observational testing. These could identify with the market structure, the three streams or the specifics of the business as appropriate to this system.

3.12 Glossary

Wholesaler: A man or organization that purchases products in extensive amounts from different merchants with the aim of offering them to affiliates who then offer to direct to customer. Merchants and wholesalers more often than not cooperate as channel accomplices.

Maker: A man or organization that makes products available to be purchased.

3.13 Answers to Self Learning Exercise

Q.1 (c)

Q.2 (a)

Q.3 (b)

Q.4 (c)

3.14 Exercise

Q.1 Write short notes on about B2C model?

Q.2 Explain the different models of E-Commerce?

Q.3 Write short notes on B2B model?

Q.4 Explain credit model?

Q.5 Explain online marketplace?

References and Suggested Readings

1. Internet Commerce: Digital Models for Business, Lawrence et. al, Wiley
2. Electronic Commerce: A Manager's Guide, Kalakota et. al, Addison-Wesley

UNIT-4
Network Infrastructure for E-Commerce

Structure of the Unit

4.0 Objective

After going through this unit, you will be able to

- Define what is E-commerce
- Discuss the applications of E-commerce
- Discuss the types of E-commerce
- List the modes of payments involved in E-commerce

4.1 Introduction

The cutting edge for business today is Electronic Commerce (E-commerce). Most people think E-commerce means online shopping. But Web shopping is only a small part of the E-commerce picture. The term also refers to online stock, bond transactions, buying and downloading software without ever going to a store. In addition, E-commerce includes business-to-business connections that make purchasing easier for big corporations. It is generally described as a method of buying and selling products and services electronically. The main Network Infrastructure of E-commerce remains the Internet and the World Wide Web, but use of email, fax, and telephone orders is also prevalent.

Figure 4.1: Online Shopping is key feature of E-Commerce

4.2 What Is E-Commerce ?

E-commerce is the application of communication and information sharing technologies among trading partners to the pursuit of business objectives. E-Commerce can be defined as a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery. E-commerce is associated with the buying and selling of information, products and services via computer networks. Key element of e-commerce is information processing through a efficient network infrastructure.

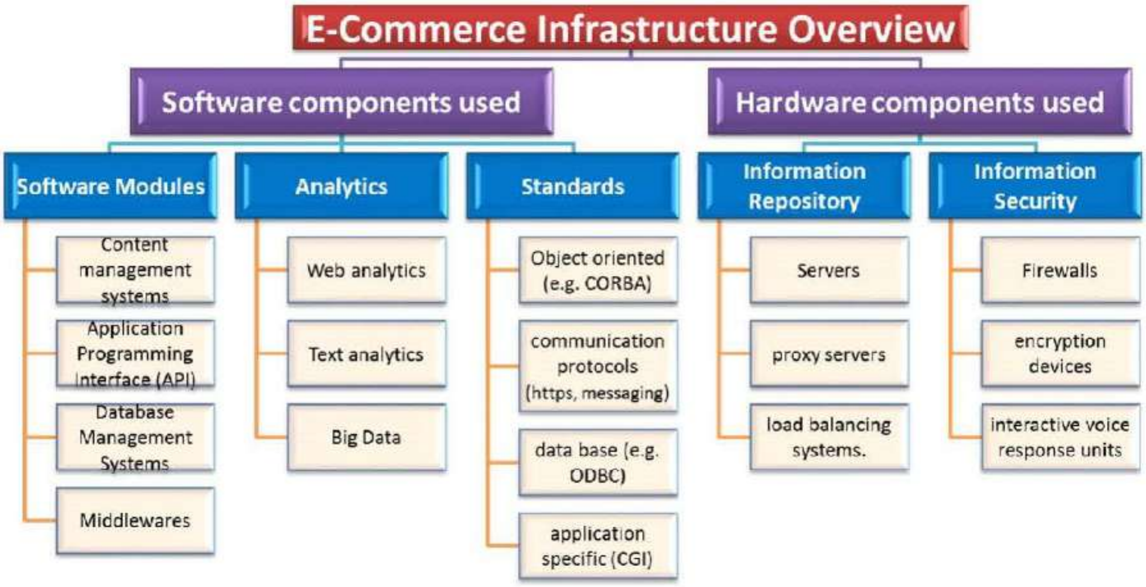


Figure 4.2: Different sections of E-commerce infrastructure

The effects of e-commerce are already appearing in all areas of business, from customer service to new product design. It facilitates new types of information based business processes for reaching and interacting with customers – online advertising and marketing, online order taking and on-line customer service etc. It can also reduce costs in managing orders and interacting with a wide range of suppliers and trading partners, areas that typically add significant overhead to the cost of products and services. Virtual network infrastructure is developed with business arrangements in which trading partners separated by geographic maps for location, easy payment methodology and expertise are able to engage in complex joint business activities, as if they were a single enterprise.

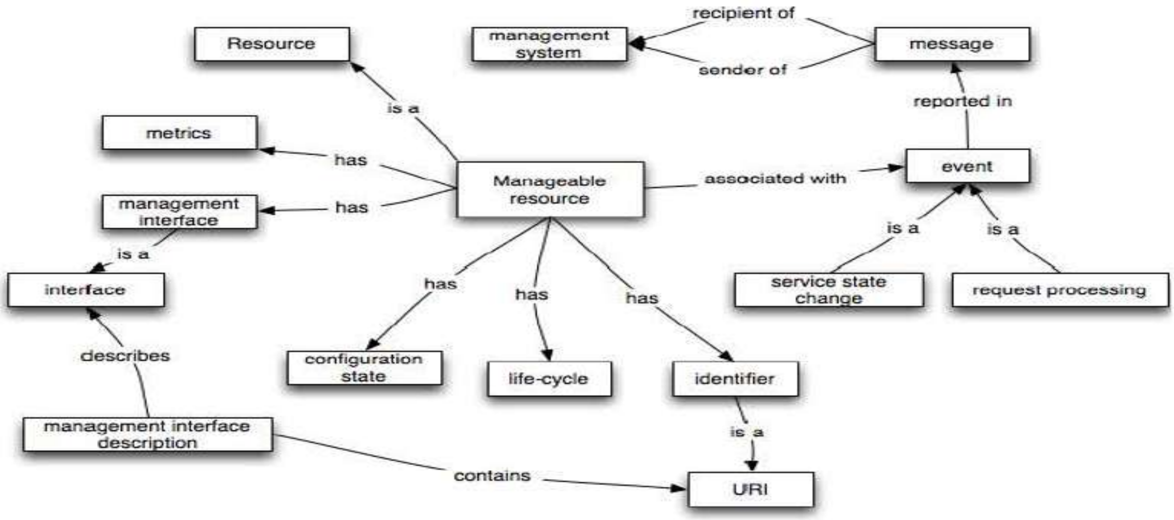


Figure 4.3: E-commerce infrastructure and technologies

4.3 Information Superhighway (I-Way)

Any successful E-commerce application will require the I-Way infrastructure in the same way that regular commerce needs the interstate highway network to carry goods from point to point. A myriad of computers, communications networks, and communication software forms the nascent Information Superhighway (I-Way). I-Way is not one monolithic data highway designed according to long-standing, well-defined rules and regulations based on well-known needs. The I-Way will be a mesh of interconnected data highways of many forms: telephone wires, cable TV wires, radio-based wireless-cellular and satellite. The I-Way is quickly acquiring new on-ramps and even small highway systems.

4.4 Consumer Oriented E-Commerce Applications

The wide range of applications for the consumer marketplace can be broadly classified into following sectors:

1) **Entertainment:** Movies on demand, video cataloging, interactive ads, multi-user games, on-line discussions.

2) **Financial services and information:** Home banking, financial services, financial news.

3) **Essential services:** Home shopping, electronic catalogs, telemedicine, remote diagnostics.

4) **Educational and training:** Interactive education, video conferencing, on-line databases.

4.5 Building Blocks In the Infrastructure of E-Commerce Applications

None of the applications would be possible without each of the building blocks in the infrastructure which are given as follows:

Common business services, for facilitating the buying and selling process.

- Messaging and information distribution, as a means of sending and retrieving information.
- Multimedia content and network publishing, for creating a product and a means to communicate about it.
- The I-Way is the very foundation for providing the highway system along which all E-commerce must travel.

4.6 Pillars Supporting the E-Commerce Applications

There are two pillars supporting all E-commerce applications and infrastructure. They are:

1. **Public policy**– To govern such issues as Universal access, privacy and information pricing.

2. **Technical standards**– To dictate the nature of information publishing, user interfaces, and transport in the interest of compatibility across the entire network.

4.7 Benefits of E-Commerce

- Electronic Commerce can offer both short term and long-term benefits to the companies. Not only can it open new markets, enabling you to reach new customers, but it can also make it easier and faster for existing customer base.
- Moving business practices, Such as ordering, invoicing and customer support, to network-based system can also reduce the paperwork involved in business-to-business transactions.

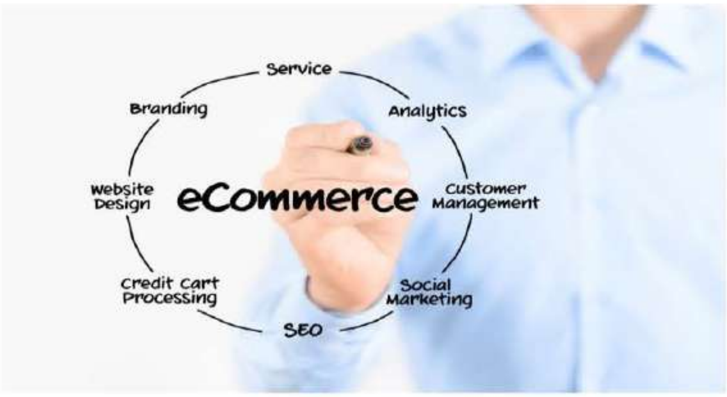


Figure 4.4: Cycle of E-Commerce

- When more of the information is digital, one can better focus on meeting your customer's needs.
- Tracking customer satisfaction, requesting more customer feedback, and presenting custom solutions for the clients are just some of the opportunities that can stem from E-commerce.

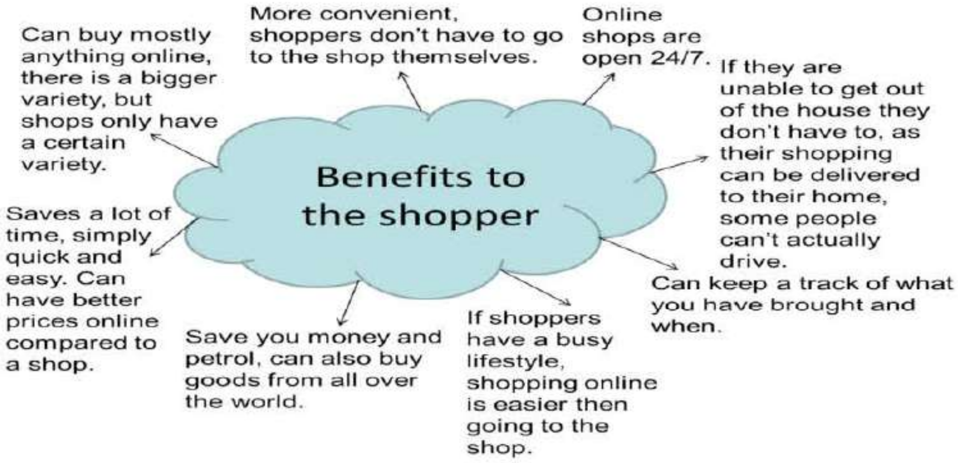

Benefits to the shopper
Can buy mostly anything online, there is a bigger variety, but shops only have a certain variety.
More convenient, shoppers don't have to go to the shop themselves.
Online shops are open 24/7.
If they are unable to get out of the house they don't have to, as their shopping can be delivered to their home, some people can't actually drive.
Can keep a track of what you have brought and when.
If shoppers have a busy lifestyle, shopping online is easier then going to the shop.
Save you money and petrol, can also buy goods from all over the world.
Saves a lot of time, simply quick and easy. Can have better prices online compared to a shop.

Figure 5.5: Benefits of E-commerce in life style

4.8 Multimedia Content for E-Commerce Applications

The technical definition of network infrastructure in terms of multimedia is the use of digital data in more than one format, such as the combination of text, audio, video and graphics in a computer file/document. Its purpose is to combine the interactivity of a user-friendly interface with multiple forms of content. E-commerce requires robust servers to store and distribute large amounts of digital content to consumers. Theses servers must handle large-scale distribution, guarantee security and complete reliability.

4.9 Client-Server Architecture in E-Commerce

All E-commerce applications follow the client-server network model. Clients are the devices plus software that request information from servers. Servers are the computers which server information upon the request by the clients. Client devices handle the user interface.

The server manages application tasks, handles storage and security and provides scalability (ability to add more clients as needed for serving more customers). The client-server architecture links PC's to a storage (or database) server, where most of the computing is done on the client.

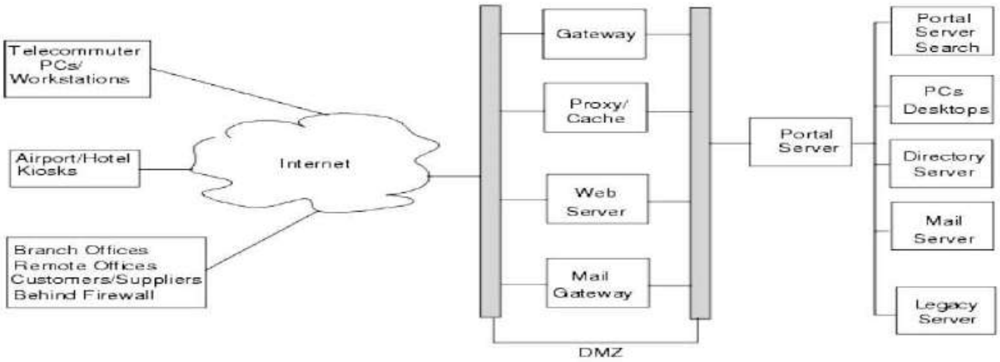
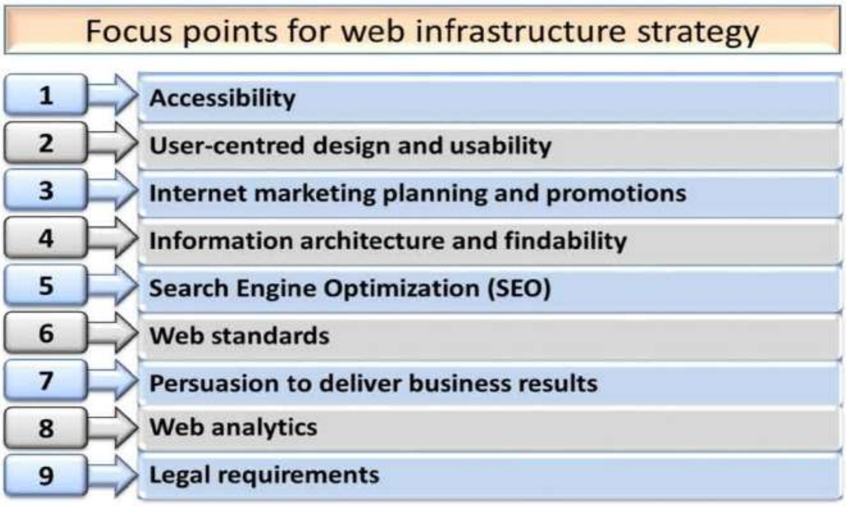


Figure 4.6: Client – Server Functioning Architecture in E-Commerce

The client-server model allows the client to interact with the server through a request-reply sequence governed by a paradigm known as message passing. Commercial users have only recently begun downsizing their applications to run on client-server networks, a trend that E-commerce is expected to accelerate.

4.10 Network Infrastructure of E- Commerce



Focus points for web infrastructure strategy

1 Accessibility

2 User-centred design and usability

3 Internet marketing planning and promotions

4 Information architecture and findability

5 Search Engine Optimization (SEO)

6 Web standards

7 Persuasion to deliver business results

8 Web analytics

9 Legal requirements

Figure 4.7:E-Commerce Infrastructure Strategy

4.10.1 Long-Distance Phone Lines

Long distance the phone network is given via cable by the between trade transporters. Long separation cell systems are utilizing the Wi-Fi innovations to join the customers around the world.

4.10.2 Satellite Systems

It assumes an essential part in the correspondence business. They have points of interest over the physical systems in that they are open for any purpose of the globe. They can give broadband advanced administrations to numerous focuses without the expense of obtaining wire/link establishment. And they can add accepting and sending locales without noteworthy extra expenses. The telecommunication systems have turned into the essential establishment for the I-way for the most part for two reasons:

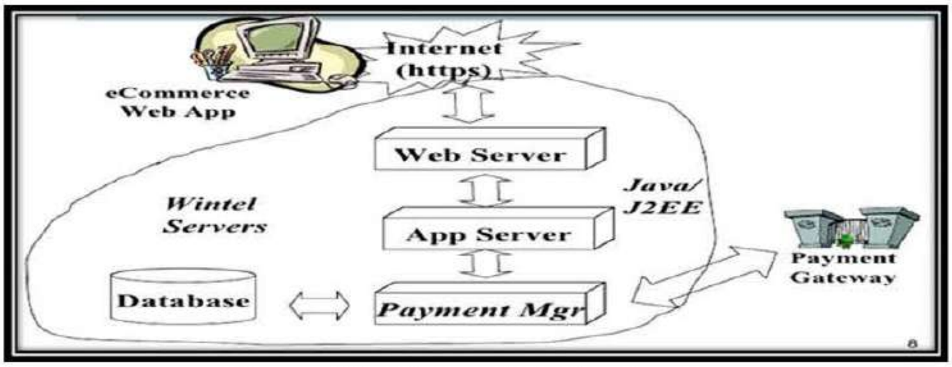


Figure 4.8: Network Infrastructure

4.10.3 Market Forces Behind I-Way

A group of PCs, systems, networks, and programs frames the incipient "Information Superhighway (I-Way)."These new thoughts request radical changes in the outline of the whole business process. I-Way is not one solid information roadway outlined by standing, very much characterized rules and regulations in light of surely understood needs. I-Way will be a cross section of interconnected information expressways of numerous structures: digital TV wires, phone wires, radio-based remote satellite, andcell phone. I-Way is rapidly gaining new entrance grades and even limited roadway frameworks. Framework base is required to transport content for e-commerce throughout the world. The automatic electronic pipeline method used to move content if there ought to emerge an event of e-commerce.

4.10.4 Component of I Way

4.10.4.1 Consumer access equipment: These are gadgets appropriated to utilize the sound and media intuitive substance of e-commerce.

4.10.4.2 Local or access road: This fragment of I-way rearranges linkages between organizations, institutes, and homes to the correspondences point. There are four distinct sorts of supplier of this segment as follows: Cable TV-based, Telecom based, Computer-based, Wireless-based network.

4.10.4.3 Global information distribution networks: It addresses to the frameworks that are connected to several nations. A large portion of the foundation for the I-way as of now exists in the limitless system of fiber optic, coaxial links, radio waves, satellites, and copper wires. Connecting every one of the parts of the I-way will require expansive capital interests in "open" frameworks and between operable hardware that uses basic models and introducing portals between different systems.

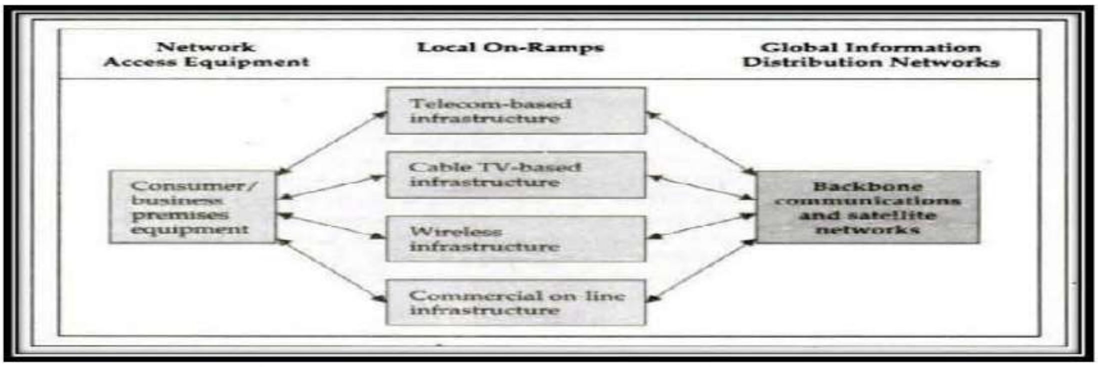

Network Access Equipment
Local On-Ramps
Global Information Distribution Networks
Telecom-based infrastructure
Cable TV-based infrastructure
Wireless infrastructure
Commercial on-line infrastructure
Consumer/ business premises equipment
Backbone communications and satellite networks

Figure 4.9: Components of the I-way

4.11 Access Equipment

It addresses a basic class, the nonattendance or moderate advancement of which is holding up different portions of the I-way. This portion of the I-way incorporates equipment and programming sellers, who give physical gadgets, for example, switches and routers, access gadgets, for example, PCs, set-top boxes, programs and working frameworks.

4.12 Global Information

It is the foundation that is joining several nations. “Extranets” utilize the web as a system to connect with these groups. An organization normally hosts various committed extranets for various groups depending on the data needs and nature of the relationship. These can some of the time also be regarded as a development of the organization "intranet" system where outside audiences are brought into the enclosure of the organization's separate operation with entrance to distinct fields or data.

4.13 Distribution Network

4.13.1 Intranet

It is a framework that is not available to the outside world of the "Intranet." If this framework is connected to the "Internet", then it will live behind a "firewall." This firewall controls access to the Intranet and Internet permits to get to the Intranet to those people who are people from the same association or affiliation.

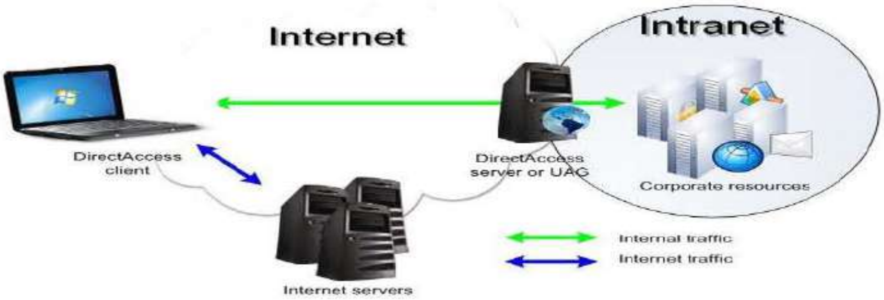


Figure 4.10: Intranet Service for Business

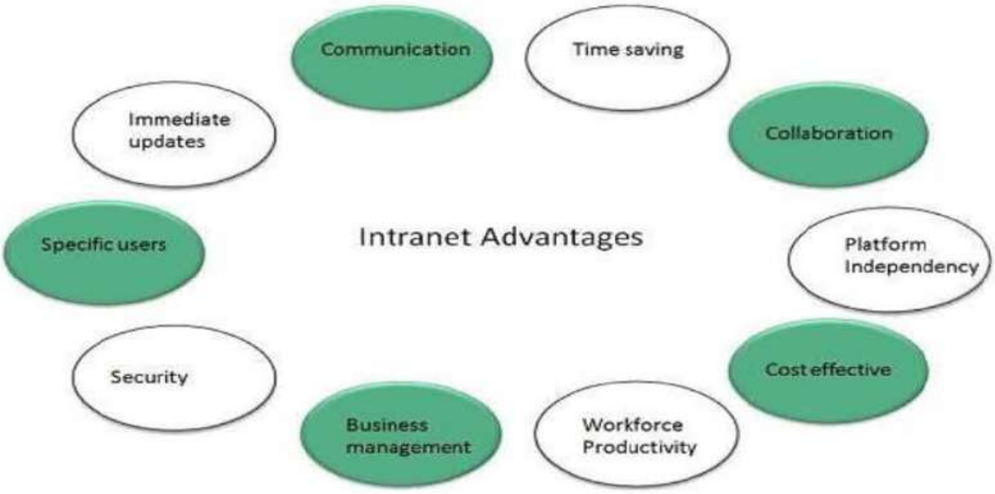


Figure 4.11: Intranet Service facilities for Business

4.13.2 Extranet

It is likewise a kind of an intranet that is accessible to endorsed outcasts. The certified server will live behind a firewall. The firewall controls access to the "Intranet and Internet is permitting access to the Intranet to those people who are completely endorsed by the organization.

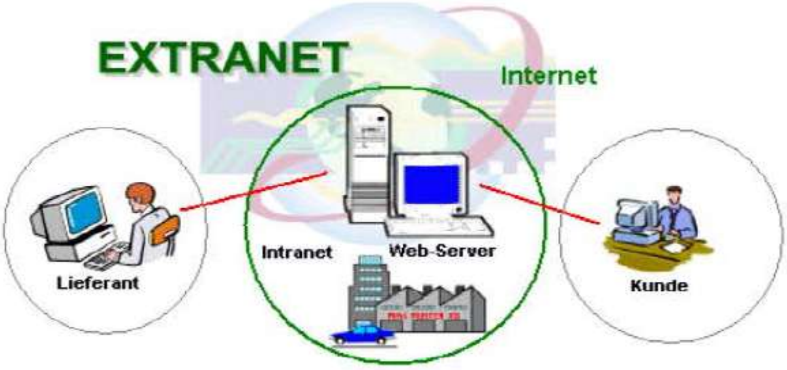


Figure 4.12: Extranet Service facilities for Business

4.13.3 Broadband Telecommunication

This system outline can be utilized to transfer voice and information over copper phone lines. Broadband telecommunications have two types which are used in house to access the Internet. First one is the "DSL (Digital Subscriber Line)." It is offered by various phone administration suppliers and takes into consideration the fast transmission of information over customary telephone lines.

The second solution is the "cable network." This methodology creates it conceivable to appreciate a percentage of the quickest voice and information correspondences conceivable while additionally building up an association with a digital TV supplier. A large number of these suppliers now utilize broadband to offer packaged administrations to clients that incorporate home phone administration. It also provides the Internet service and access to satellite TV. A solitary connection into the home builds up the system for each purpose which is a part of network infrastructure.

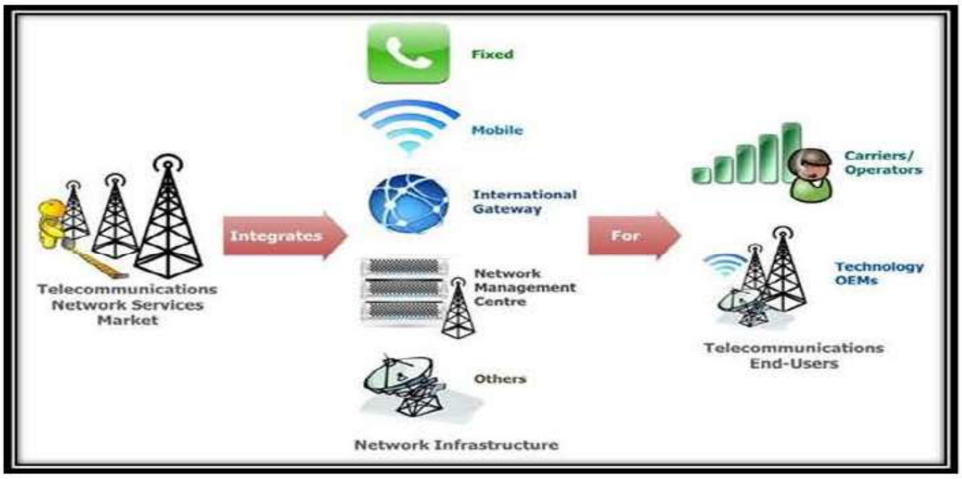


Figure 4.13: Structure of Broadband Telecommunication

4.14 Types of E-Commerce

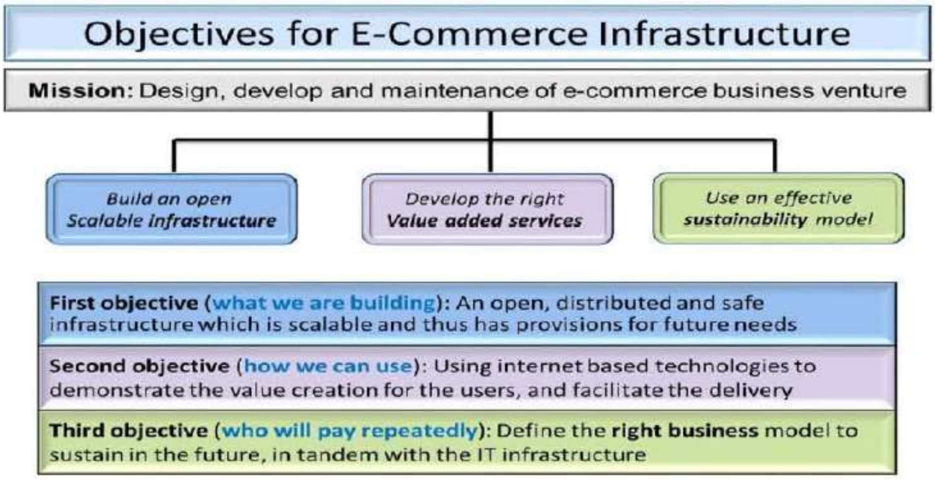
The following three strategies are the focal points for E-Commerce:-

4.14.1 Business-to-business E-commerce: The Internet can connect all businesses to each other, regardless of their location or position in the supply chain.

4.14.2 Business-to-consumer E-commerce: It is a One-way marketing process. Corporate web sites are still prominent distribution mechanisms for corporate brochures, the push, one-way marketing strategy.

4.14.3 Purchasing over the Web: Availability of secure web transactions is enabling companies to allow consumers to purchase products directly over the web. Electronic catalogs and virtual malls are becoming commonplace.

4.14.4 Relationship Marketing: The most prominent of these new paradigms is that of relationship marketing. Because consumer actions can be tracked on the web, companies are experimenting with this commerce methodology as a tool for market research and relationship marketing: Consumer survey forms on the web, Using web tracking and other technology to make inferences about consumer buying profiles, Customizing products and services, Achieving customer satisfaction and building long-term relationships.



Objectives for E-Commerce Infrastructure

Mission: Design, develop and maintenance of e-commerce business venture

Build an open Scalable infrastructure
Develop the right Value added services
Use an effective sustainability model

First objective (what we are building): An open, distributed and safe infrastructure which is scalable and thus has provisions for future needs

Second objective (how we can use): Using internet based technologies to demonstrate the value creation for the users, and facilitate the delivery

Third objective (who will pay repeatedly): Define the **right business** model to sustain in the future, in tandem with the IT infrastructure

Figure 4.14: E-Commerce Infrastructure Objectives

4.14.5 Intra-Company E-Commerce: Companies are embracing intranets at a phenomenal growth rate because they achieve the following benefits:

Reducing cost- lowers print-intensive production processes, such as employee handbooks, phone books, and policies and procedures.

Enhancing communications- effective communication and training of employees using web browsers builds a sense of belonging and community.

Distributing software- upgrades and new software can be directly distributed over the web to employees.

Sharing intellectual property- provides a platform for sharing expertise and ideas as well as creating and updating content - "Knowledge webs". This is common in organizations that value their intellectual capital as their competitive advantage.

Testing products- allows experimentation for applications that will be provided to customers on the external web.

4.15 Technologies of E-Commerce

While many technologies can fit within the definition of "Electronic commerce," the most important are:

Electronic Data Interchange (EDI)

EDI is the computer-to-computer exchange of structured business information in a standard electronic format. Information stored on one computer is translated by software programs into standard EDI format for transmission to one or more trading partners. The trading partners' computers, in turn, translate the information using software programs into a form they can understand.

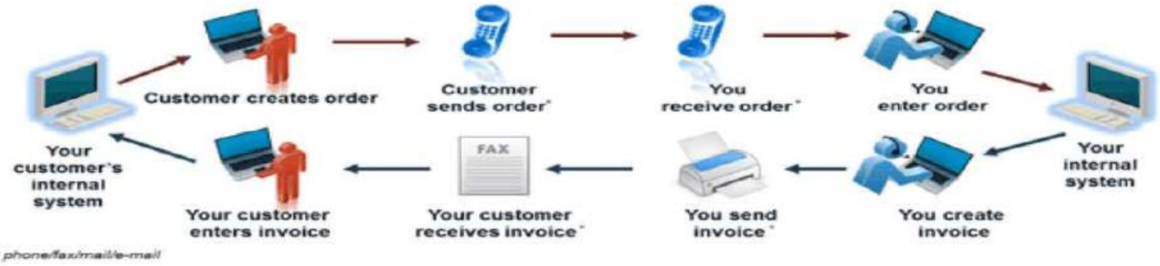


Figure 4.16 Manual work flow of Electronic Data Interchange (EDI)

Bar Codes

Bar codes are used for automatic product identification by a computer. They are a rectangular pattern of lines of varying widths and spaces. Specific characters (e.g.

numbers 0-9) are assigned unique patterns, thus creating a "font" which computers can recognize based on light reflected from a laser.

Electronic Mail

Messages composed by an individual and sent in digital form to other recipients via the Internet.

Internet

The Internet is a decentralized global network of millions of diverse computers and computer networks. These networks can all "talk" to each other because they have agreed to use a common communications protocol called TCP/IP. The Internet is a tool for communications between people and businesses. The network is growing very fast and more people are gaining access to the Internet, it is becoming more and more useful.

World Wide Web

The World Wide Web is a collection of documents written and encoded with the Hypertext Markup Language (HTML). With the aid of a relatively small piece of software (called a "browser"), a user can ask for these documents and display them on the user's local computer, although the document can be on a computer on a totally different network elsewhere in the world. HTML documents can contain many different kinds of information such as text, pictures, video, sound, and pointers, which take users immediately to other web pages.

Product Data Exchange

Product data refers to any data that is needed to describe a product. Sometimes that data is in graphical form, as in the case of pictures, drawings and CAD files.

Electronic Forms

Electronic forms are a technology that combines the familiarity of paper forms with the power of storing information in digital form. Imagine an ordinary paper form, a piece of paper with lines, boxes, check-off lists, and places for signatures. To the user an electronic form is simply a digital analogue of such a paper form, an image, which looks like a form but which appears on a computer screen and is filled out via mouse, and keyboard. Behind the screen, however, lie numerous functions that paper and pencil cannot provide. Those extra functions come about because the data from electronic forms are captured in digital form, thus allowing storage in data bases, automatic information routing, and integration into other applications.

4.16 Electronic Shopping Cart

An electronic shopping cart works the same way a shopping cart does in the physical world. As you browse through an online store, you can place products in your virtual shopping cart, which keeps track of the products you have placed in it. When you're ready to leave the store, you click a "check out" link that shows you what you've placed in your virtual shopping cart. You can usually remove items that you're no longer interested in purchasing and then enter your shipping and payment information to process your order.

Figure 4.17: Electronic Cart Facility of E-commerce

4.17 Is E-Commerce Safe ?

No e-commerce system can guarantee 100-percent protection for your credit card, but you're less likely to get your pocket picked online than in a real store. Consumers don't really believe it yet, but experts say E-commerce transactions are safer than ordinary credit card purchases. Microsoft Internet Explorer, or other sites transactions can be encrypted using Secure Sockets Layer, a protocol that creates a secure connection to the server, protecting the information as it travels over the Internet. SSL uses public key encryption, one of the strongest encryption methods around. Browser makers and credit card companies are promoting an additional security standard called Secure Electronic Transactions (SET). SET encodes the credit card numbers that sit on vendors' servers so that only banks and credit card companies can read the numbers.

4.18 Systems of Payments in E-Commerce

E-commerce is rife with buzzwords and catchphrases. Here are some of the current terms people like to throw around:

4.18.1 Credit Card-Based: If consumers want to purchase a product or service, they simply send their credit card details to the service provider involved and the credit card organization will handle this payment like any other.

4.18.2 Smart Cards: These are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe.

1) **Relationship based smart credit cards**: This is an enhancement of existing card services and/or the addition of new services that a financial institution delivers to its customers via a chip-based card or other device. These new services may include access to multiple financial accounts, value-added marketing programs, or other information cardholders may want to store on their card.

2) **Electronic Purses:** These are wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything from buying food to paying subway fares.

4.18.3 Digital or Electronic Cash: Also called e-cash, these terms refer to any of several schemes that allow a person to pay for goods or services by transmitting a number from one computer to another. The numbers, just like those on a dollar bill, are issued by a bank and represent specified sums of real money. One of the key features of digital cash is that it's anonymous and reusable, just like real cash. This is a key difference between e-cash and credit card transactions over the Internet.

4.18.4 Electronic Cheque: Currently being tested by Cybercash, electronic checking systems such as PayNow take money from users' checking accounts to pay utility and phone bills.

4.18.5 Electronic Wallet: This is a payment scheme, such as Cybercash's Internet Wallet, that stores your credit card numbers on your hard drive in an encrypted form. You can then make purchases at Web sites that support that particular electronic wallet. When you go to a participating online store, you click a Pay button to initiate a credit card payment via a secure transaction enabled by the electronic wallet company's server. The major browser vendors have struck deals to include electronic wallet technology in their products.

4.19 Self Learning Exercise

Q.1 Which of the following is not an scripting language?

a) HTML

b) XML

c) Postscript

d) Javascript

Q.2 A digital signature is

a) scanned signature

b) signature in binary form

c) encrypting information

d) handwritten signature

Q.3 A computer communication technology that provides a way to interconnect multiple computer across short distance is

a) LAN

b) MAN

c) WAN

d) Wireless network

Q.4 Telnet is a service that runs

a) Television on net

b) Remote program

c) Cable TV network

d) Telenext

Q.5 A device that forwards data packet from one network to another is called a

a) Bridge

b) Switch

c) Hub

d) Gateway

4.20 Summary

E-commerce is a new way of conducting, managing and executing business transactions using computer and telecommunications networks. As awareness of the Internet throughout the commercial world and general public increases, competitiveness will force lower entry barriers, continued rapid innovation and expansion of markets. The real key to making electronic commerce over the Internet a normal, everyday business activity is the convergence of the telecommunications, content/media and software industries. E-Commerce is expected to improve the productivity and competitiveness of participating businesses by unprecedented access to an on-line global market place with millions of customers and thousands of products and services.

4.21 Glossary

CGI script: Common gateway Interface is a scripting system designed to work with HTTP Web Servers. The scripts, usually written in the Perl coding language, are ofter used to exchange data between a Web server and databases.

Digital Cash: An electronic replacement of cash.

Joint Electronic Payments Initiative (JEPI): This initiative, led by the World Wide Web Consortium and Commerce Net, is an attempt to standardize payment negotiations. On the buyer's side (the client side), JEPI serves as an interface that enables a Web browser, and wallets, to use a variety of payment protocols. On the merchant's side (the server side), JEPI acts between the network and transport layers to pass off the incoming transactions to the proper transport and payment protocols.

Microcash: Small denomination digital tokens.

Micro transactions: Low-cost, real-time transactions using micro cash.

Smart cards: A credit card-sized plastic card with a special type of integrated circuit embedded in it. The integrated circuit holds information in electronic form and controls who uses this information and how.

Tokens: Strings of digits representing a certain amount of currency. The issuing bank validates each token with a digital stamp.

Value added networks: Networks that are maintained privately and dedicated to EDI between business partners.

4.22 Answers to Self Learning Exercise

Q.1 (c)

Q.2 (c)

Q.3 (a)

Q.4 (b)

Q.5 (b)

4.23 Exercise

Q.1 Write a short note on cloud computing.

Q.2 Explain the working of payment methodology be electronic cheque.

Q.3 Discuss SET protocol works for networking in e-commerce.

Q.4 Discuss the work flow of Electronic Cart facility.

Q.5 Discuss Intranet and Extranet uses in E- commerce.

References and Suggested Readings

1. Ravi Kalakota, Andrew b.Whinston, Frontiers of Electronic Commerce, Awl International.
2. Bajaj KK and Nag Debjani, From EDI to Electronic Commerce, TataMcGraw-Hill.
3. Bajaj and Nag, Electronic Commerce: The cutting edge of Business, Tata Mcgraw-Hill.
4. Greg Holden, Starting An E-commerce Business For Dummies, Second edition,IDG books India.
5. David Kosiur, Understanding Electronic Commerce, Microsoft Press.

UNIT-5

Mobile Commerce

Structure of the Unit

5.0 Objective

In this chapter we shall focus upon the following topics:

- Mobile Commerce
- History of M-commerce
- Advantages and Disadvantages of M-commerce
- M-commerce vs E-commerce
- Mobile Computing Application
- Wireless Application Protocols (WAP)

- WAP architecture
- WAP technology
- Mobile Information Devices
- Security issues

5.1 Introduction

Mobile Commerce in general can be understood as buying and selling of products or services using wireless mobile devices like a mobile phone , smartphone , tablet , Personal Digital Assistant (PDA) , smart wearable's etc. The technology behind M-Commerce is based on Wireless Application Protocol (WAP), and is expected to surpass E-commerce as the choice for online transactions very soon.

The value of m-Commerce industry as on 2016 is estimated to be roughly around 230 billion USD and is expected to grow to 700 billion USD by the end of 2017 worldwide.

India and other Asian countries together contributes to almost 50% of this economy, and with still a large part of population to be covered , this segment has real promise in developing countries .

India has almost 46 crore people connected to internet (December 2016) and is expected to grow to 75 crore by the end of 2020 and the potential India holds has really drawn attention of major smartphone companies like Samsung , Motorola , Micromax and many others to make smartphones keeping Indians as major point of their business .

The competition is just not amongst mobile devices provider, but there exists a cut throat competition amongst Internet Service Provider (ISP) too for customer acquisition. The recent major example is of Lyf smartphones founded by Reliance JioInfocomm Limited (RJIL) and Reliance Jio SIM which offered free calling, free data and successfully acquired over 50 million customers. It is backed by Reliance Group and has invested funding in this sector that no company ever had invested in globally, giving people access to data at cheapest price.

In order to exploit the potential mobile commerce market, mobile phone manufacturers such as Nokia, Ericsson, Motorola, and Qualcomm are working with carriers such as AT&T Wireless and Sprint to develop WAP-enabled smartphones. Smartphones offer fax, e-mail, and phone capabilities in addition to basic phone abilities like calling etc.

Since the launch of the iPhone, mobile commerce has moved away from SMS systems and into actual applications. SMS has significant security vulnerabilities and congestion problems, even though it is widely available and accessible. In addition, improvements in the capabilities of modern mobile devices make it prudent to place more of the resource burden on the mobile device.

The major areas affected by m-Commerce is:

- **Financial services**, such as mobile banking, mobile brokerage,and money transfer etc.
- **Information services,** such as news updates, match scores, traffic updates, weather forecasts etc.
- **Services,** such as hiring taxi, booking tickets, hotels etc.
- **Retail,** such as buying products online, ordering food online etc.

5.2 History of M - Commerce

The term mobile commerce was first phrased by Kevin Duffey on 10th November 1997, at the launch of Global Mobile Commerce forum, where he was elected as Executive Chairman, by which he meant "the delivery of electronic commerce capabilities directly into the consumer's hand, anywhere, via wireless technology."

Mobile commerce services were first delivered in 1997, when the first two mobile-phone enabled Coca Cola vending machines were installed in the Helsinki area in Finland. The machines accepted payment via SMS text messages. This work evolved to several new mobile applications such as the first mobile phone-based banking service was launched in 1997 by Merita Bank of Finland, also using SMS. Finnair mobile check-in was also a major milestone, first introduced in 2001

The m-Commerceserver was developed in late 1997 by Kevin Duffey and Andrew Tobin at Logicawhich won the 1998 Financial Times award for "most innovative mobile product," in a solution implemented with De La Rue, Motorola and

Logica.The Financial Times commended the solution for "turning mobile commerce into a reality."The trademark for m-Commerce was filed on 7 April 2008.

In 1998, the first sales of digital content as downloads to mobile phones were made possible when the first commercial downloadable ringtones were launched in Finland by Radiolinja (now part of Elisa Oyj).Mobile-commerce-related services spread rapidly in early 2000. Austria started offering train ticketing via mobile device. Japan also offered mobile purchases of airline tickets.

In April 2002, building on the work of the Global Mobile Commerce Forum (GMCF), the European Telecommunications Standards Institute (ETSI) appointed Joachim Hoffmann of Motorola to develop official standards for mobile commerce.PDAs and cellular phones have become so popular that many businesses (Flipkart, Ola, Olx and Banks) are beginning to use mobile commerce as a more efficient way to communicate with their customers.

5.3 Advantages and Disadvantages of M - Commerce

Advantages of Mobile Commerce:

This mCommerce is beneficial for both types of businesses large scale and small scale. The mobile users increase day by day, so through mCommerce, business gets large and growing market place for the wide range of goods and services.

1. ***Cover Widedistance***: Mobile is the only technology which has now become almost an inseparable part of any person's social and business life, much more common than traditional computers. So, it is easy to reach users through mCommerce.
2. ***Consumer Deals:*** As more users use mCommerce, there are lots of companies use the mCommerce platform to reach customers by tempting them with different and better deals in comparison to their competitor.
3. ***Savings:*** Companies are expanding their reach to the consumer directly through mCommerce, so users don't have to go to the store physically and at the end it saves user's time and money. Example are companies like amazon, Flipkart etc.

4. ***Easy to use:*** There is no need of the skilled consumer. Buyers can have look thousands of items on their cell phones and there is no need of online checkout process. Most of the companies invest heavily on keeping their site / apps experience easy and delightful.

Disadvantages of Mobile Commerce:

Every invention has its own merits and demerits. It is applicable in this mCommerce business also.

1. ***Smartphone Limitation:*** Mobile has no big screen like desktop or laptops, so sometimes users try to navigate more and more to choose just one item from thousands. It affects shopping rates.
2. ***Habituate:*** Every new technology has some problem at the initial phase. Since mCommerce is a new application, so sometimes people hesitate to accept itas they are habituated to buy products from physical stores or e-commerce.
3. ***Risk Factor:*** Each business has its own risk. Same Mobile commerce is the growing field and a lot of investment in this field becomes risky. Because technology changes day by day. Moreover, there less security in the wireless network, so in data transfer hacking chances are more.
4. ***Connectivity:*** Connectivity is generally not available in all areas, and in areas in which it is available connection speedbecomes an issue. It quite often become hectic for the user to go through entire product purchase process.

5.4 M-Commerce vs. E -Commerce

The major differences between e-commerce and m-commerce are explained below:

1. E-commerce is defined as the performance of business activities with the use of the internet. When any sort of commercial transaction is transacted / initiated with the use of mobile cellular devices, it is known as m-commerce.
2. E-commerce originated in 1970s while m-commerce originated in 1990s.

3. M-commerce was originally developed on the lines of e-commerce. So it can be said that m-commerce is a subset of e-commerce.

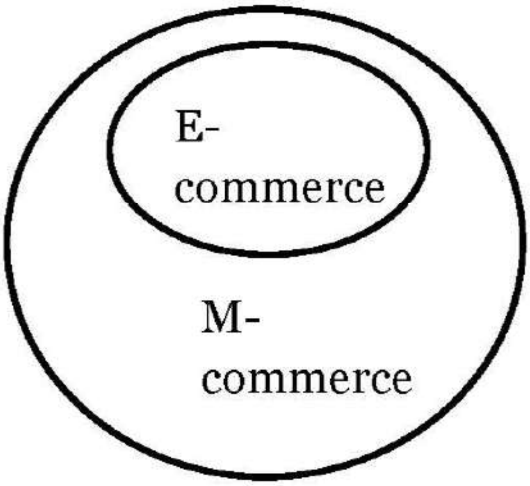


Figure 5.1

4. E-commerce activities are concluded with the help of computers and laptops, whereas in m-commerce, smartphones, tablets, iPad, PDA's (Personal Digital Assistant), etc. are used.

5. In e-commerce, the use of the internet is compulsory but in the case of m-commerce the use of the internet is not mandatory. For example native apps for android and iOS doesn't compulsorily require internet, it also doesn't require continuous electricity because of inbuilt rechargeable batteries.

6. The connectivity of m-commerce is comparatively larger than e-commerce.

7. M-commerce devices are easy to carry anywhere because they are light weighted which is not possible with e-commerce.

5.5 Mobile Computing Application

Mobile computing refers to the use of small and portable computing device in wireless enabled networks that provides wireless connections.

Mobile computing finds its application in following trending market:

3G:

3G or third generation mobile telecommunications is a generation of standards for mobile phones and mobile telecommunication services fulfilling the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union. Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.

Global Positioning System (GPS):

The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites. The GPS program provides critical capabilities to military, civil and commercial users around the world. In addition, GPS is the backbone for modernizing the global air traffic system, weather, and location services.

Long Term Evolution (LTE):

LTE is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using new modulation techniques. It is related with the implementation of fourth Generation (4G) technology.

WiMAX:

WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the latest update providing up to 1 Gbit/s for fixed stations. It is a part of a fourth generation or 4G wireless-communication technology. WiMAX far surpasses the 30-metre wireless range of a conventional Wi-Fi Local Area Network (LAN), offering a metropolitan area network with a signal radius of about 50 km. WiMAX offers data transfer rates that can be superior to conventional cable-modem and DSL connections, however, the bandwidth must be shared among multiple users and thus yields lower speed in practice.

Near Field Communication:

Near Field Communication (NFC) is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimetres. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-

Fi. Communication is also possible between an NFC device and an unpowered NFC chip, called a "tag".

Today's computing has rapidly grown from being confined to a single location. With mobile computing, people can work from the comfort of any location they wish to as long as the connection and the security concerns are properly factored. In the same light, the presence of high speed connections has also promoted the use of mobile computing.

Being an ever growing and emerging technology, mobile computing will continue to be a core service in computing, and Information and Communications Technology.

5.6 Wireless Application Protocols (WAP)

Wireless Application Protocol (WAP) is an open specification that offers a standard method to access internet based content and services from wireless devices. A **WAP browser** is a web browser for mobile devices such as mobile phones that uses the protocol and connects to the WAP gateway and make requests for information from web servers in the normal form of a content that must be formatted suitably for small screens and low bandwidth and high latency connection. It used content written in Wireless Mark-up Language (WML). Before the introduction of WAP, mobile service providers had limited opportunities to offer interactive data services, but needed interactivity to support Internet and Web applications such as:

- Email by mobile phone
- Tracking of stock-market prices
- Sports results
- News headlines
- Music downloads

WAP was invented and is driven by the WAP forum – a group originally formed by Nokia, Ericsson, Motorola and Phone.com.

WAP has today become an outdated technology as most modern handset internet browsers now fully support HTML , so we do not need to use WAP mark-up(

WML) for webpage compatibility, and most of them are no longer able to render and display pages written in WAP. The main advantage of it is that it is network independent and is widely accepted by handset manufacturers.

5.7 WAP Architecture

WAP architecture mimics the International Standards Organisation (ISO) Open System Interconnection (OSI) network model. The OSI model defines a layered framework for generically describing and designing protocols. The OSI model has seven layers, while WAP uses only six, but with similar approach.

Each layer has its own tasks and can interact with layer just above or below it. WAP device makes URL requests that starts at application layer and is processed until the request goes out over a bearer network to the gateway. Responses enters the device at the bearer level, and are transformed to get displayed at the application layer.

It is essential for a WAP request to be transformed into appropriate format before being sent wirelessly to a gateway and finally off to a web server, for the request to be fulfilled. The response on the return trip is decrypted and decoded before being displayed on the screen. It is necessary for request and response cycle to follow same order as in Figure.

Application Layer (WAE)		Other services and applications.
Session Layer (WSP)		
Transaction Layer (WTP)		
Security Layer (WTLS)		
Transport Layer (WDP)		
Bearers : GSM , CDMA , CDPD , Flex and many others		

Figure: 5.2

5.8 WAP Technology

AMPS

Advanced Mobile Phone Service or AMPS, operates at 800 MHz . It is voice only analog transport. It can also be used with cellular modem for circuit-switched data communications. However it has been replaced by newer technologies today.

TDMA

Time Division Multiple Access is a digital transport that divides the frequency range allotted to it into a series of channels, divided by time slots. It forms the basis of GSM. It is also possible to use TDMA on top of AMPS by converting an analog network to a hybrid analog / digital network.

CDMA

It stands for Code Division Multiple Access and is a digital transport that has been used by US military since 1940. It enables simultaneous usage 10 – 20 times of AMPS and up to three times of TDMA. It uses less power, resulting in much better battery life. It is more secure and reportedly has fewer dropped calls and better voice quality. This technology is pioneered by US based QUALCOMM.

GSM

It stands for Global System for Mobile communication, and is also known as Personal Communication Network (PCN). It started its operation in the 900 MHz frequency range. It uses all digital and is based on TDMA network. Every GSM phones can access data functions of speed up to 9600 bps, (effective throughput up to 4800 bps only). The services included are internet access without modem, SMS etc.

CDPD

Cellular Digital Packet Data or CDPD, is TCP / IP based mobile data only service that is based on AMPS networks. It requires a modem to convert the TCP / IP based data into analog signals when sending and receiving, as it runs on analog networks.

CDPD has raw throughput of 19200 bps out of which half is consumed by TCP /

IP protocol, giving us an effective data throughput of about 9600 bps. It is not so efficient and is widely replaced by digital only networks.

5.9 Mobile Access Information Devices

MAID as commonly called , Mobile Access Information Devices , in combination with Connected Limited Device Configuration (CLDC) , is the java runtime environment for today's Mobile Information Devices (MIDs) , such as phones and PDAs . It provides the core application functionality required by mobile applications – including the user interface, network connectivity, local data storage, and application lifecycle management – packaged as a standardized Java Runtime Environment and set of Java Technology APIs.

5.10 Security Issues

In the digital world security has always been a challenge. According to recent statistics hackers have had an impact on almost 90 % of small and medium scale online business as they mostly fail to handle these issues properly mostly because of lack of enough funding to afford developers or third party firewalls or at times they don't realise the need to afford such services until they are severely hit. The most common reason for attacks are access to data of users, getting price list etc., and the methods adopted by them are:

- DDoS meaning distributed denial of service attacks
- Computer viruses / worms
- Malware (malicious code)
- Phishing,
- Spam
- Identity theft
- Credit card fraud etc.

In India, ***Information Technology Act, 2000,*** contains rules against cybercrime.

There are however few ways in which we can protect ourselves from hackers. They are:

- Use latest Antivirus software
- Pay only on trusted site (site with green lock in URL bar mentioning secure)
- Insert Firewalls
- Uninstall unnecessary software
- Maintain backup
- Check security settings
- Stay anonymous - choose a genderless screen name
- Never give your full name or address to strangers
- Never do any transaction using public Wi-Fi.

5.11 Self Learning Exercise

Q.1 Who coined the term M-Commerce?

a) Jeff Bezos

b) Kevin Duffey

c) Steve Jobs

d) Marissa Mayer

Q.2 What type of Web technology creates a secure and private connection between two computers?

a) Secure Socket Layer

b) Encryption

c) Internet Locked Connections

d) Sheltered Web Apps

Q.3 What term refers to your ability to connect to the internet and your company from a wireless device?

a) Net Services

b) USSD

c) Wi-Fi

d) Mobile Computing

5.12 Summary

Mobile Commerce often referred to as m – commerce,is a part of e-commerceand has further extended its reach to wide range of users. In developing countries like India, most of the people who come online for first time uses mobile device and this trend has led companies to design their user interfaces according to mobile first technology to have fair share in the ever growing market. This segment holds huge potential as today it is amongst industry with highest growth rate.

Like any emerging market, there are however speculations about how to use this technology, while some organisations have invested to be an early bird and acquire customers with lesser competition, while others have adopted wait and see approach, and is expected to enter when they see clear profit.

The other major difference between e-commerce and m-commerce is the opportunity to connect information with objects in a more direct way that has been possible until now. This is the world predicted by Internet of Things, according to a report published by ITU (International Telecommunications Union) in 2005, where objects have life history of their own that we can use to our advantage.

Many more people have access to a mobile phone that to a computers and that means that m-commerce has the opportunity to connect not just big businesses but also small business and consumers on a massive scale. In this sense, mobile phones have potential to bridge the digital divide and allow organisations and individuals to reach out to one another more easily than ever before .

5.13 Glossary

Latency : time delay in communication between client and server

Bandwidth : Amount of data transferred per unit time.

WAP Gateway : software infrastructure for wirelessnetwork.

5.14 Answers to Self-Learning Exercise

Q.1 (b)

Q.2 (a)

Q.3 (d)

5.15 Exercise

Q.1 M-Commerce did not originate in which of the following countries?

a) Norway

b) Austria

c) United States

d) Japan

Q.2 Which of the following is not considered a device suitable for m-commerce?

a) An iPod Touch with internet access

b) Smart Phones

c) Blackberry

d) None of these

Q.3 The first company to engage in m-commerce was:

a) Pepsi

b) Coca-Cola

c) Cadbury

d) Apple

Q.4 Which of the following is not a current application of m-commerce?

a) IPhone Zagat

b) RedLaser

c) JoJo Contactless Payment service

d) Zynga Farmer Exchange

Q.5 Which of the following is not an obstacle of m-commerce?

a) Slow Connectivity

b) Security

c) Standardization

d) None of the above

Q.6 What year did m-commerce begin?

a) 1997

b) 1999

c) 1995

d) 2001

Q.7 What is the name of the European association who is standardizing m-commerce?

a) FCC

b) SimPay

c) Pay Pal

d) EU Communication Bureau

Q 8. True or False? Lufthansa Air passengers can check in and board flights with an electronic ticket on their mobile device?

a) True

b) False

5.16 Answers to Exercise

Q.1	(c)
Q.2	(d)
Q.3	(b)
Q.4	(d)
Q.5	(d)
Q.6	(a)
Q.7	(b)
Q.8	(a)

References and Suggested Readings

1. Gupta Sarika and Gupta Gaurav "E-Commerce", Second Edition.
2. Joseph P.T., S.J, "E-Commerce an Indian perspective", Third Edition.

UNIT-6

Security in E-Commerce

Structure of the Unit

6.0 Objective

In this unit we shall learn the following topics

- Client - Server Network
- Threats to Servers
- Trust-Based Security & STO
- Password Schemes & Biometric Systems

6.1 Introduction

Web based business acquaints with the exchange of items and administrations over the web. All real retail marks have web nearness, and heaps of brands haven't any related blocks and mortar nearness. Be that as it may, internet business furthermore applies to business to business exchanges, for instance, amongst creators and providers or wholesalers. Online business frameworks are applicable for the administrations exchange. For instance, on-line managing an account and business administration's empower clients to recover bank explanations on-line, exchange reserves, pay MasterCard bills, apply for and get endorsement for a substitution contract, get and offer securities, and acquire cash steerage and information. Electronic trade that is directed between organizations is said as business-to-business or B2B. B2B are frequently friendly all invested individuals (e.g. exchange merchandise trade) or confined to specific, pre-qualified members (individual electronic market). Electronic trade that is led amongst organizations and clients, on the inverse hand, is specified as business-to-shopper or B2C. This is frequently the sort of electronic trade directed by compacts like, flip truck, Amazon.com. On-line looking for could be a kind of electronic business wherever the client is specifically on-line to the merchant's PC ordinarily utilizing the web.

Figure 6.1: Secured e-Business is needed online

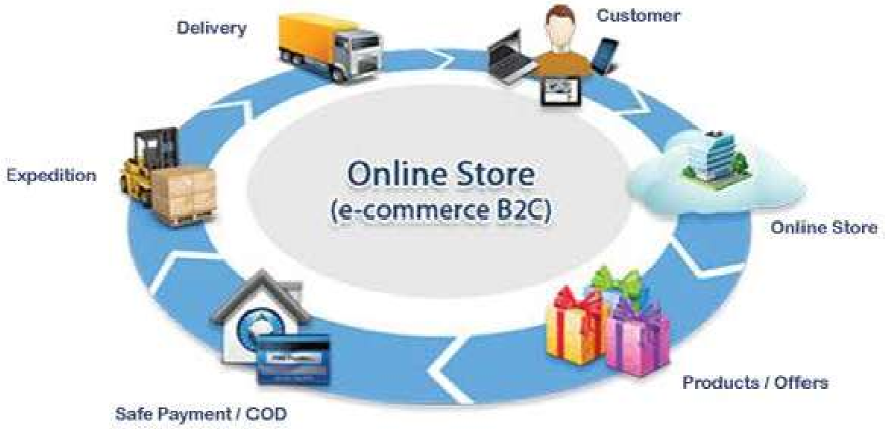


Figure 6.2: Facilities provided by online stores

There is no between go between administration. The deal and purchase dealings are finished electronically and intelligently in timeframe like Amazon.com for brand beating new books. On the off chance that an intermediates is blessing, then the deal and purchase dealings is named electronic business like eBay.com.

6.2 History

The years prior, Traditional showcasing, deals, retail, corporate business choices was not a general classification that fuses many types of promoting and advertising. It's the most conspicuous sorts of showcasing, incorporating the notices that were particularly restricted. Most conventional showcasing systems fall under one of four classes: print, communicate, post office based mail, and phone. Print advertising is the most established type of customary showcasing.

Today, print promoting as a rule alludes to publicizing space in daily papers, magazines, pamphlets, and other pieces of literature expected for conveyance.

Communicate showcasing incorporates TV and radio promotions. Radio communicates have been around since the 1900s, and the main business communicate a radio program bolstered by on-air ads broadcast on November 2, 1920. TV, the following stride in diversion innovation, was speedier to receive publicizing, with less than ten years between its origin and the primary TV advertisement in 1941 however not in India.

Standard mail showcasing utilizes printed material like postcards, leaflets, letters, indexes, and pamphlets sent through postal mail to draw in shoppers. At last,

6.3 Overview

phone showcasing, or telemarketing, is the act of conveying deals messages via telephone to persuade purchasers to purchase an item or administration. This type of promoting has turned out to be fairly questionable in the advanced age, with numerous telemarketers utilizing forceful deals strategies.

Internet business security is the assurance of online business resources from unapproved get to, utilize, adjustment, or pulverization.

1. Internet business resources
   a) Intellectual property
   b) Client PCs a push for point-and-snap business
   c) Messages going on the correspondence channel universal availability
   d) Web server and its equipment complex frameworks and systems.
2. The significance of securing online business
   a) Secrecy: security against unapproved information revelation and confirmation of information source
   b) Integrity: avoidance against unapproved information adjustment
   c) Necessity: avoidance against information deferrals or expulsion
   d) Non-renouncement: aversion against any one gathering from reneging on an understanding sometime later
   e) Protect enterprise's picture and notoriety
   f) Minimize the effect of security disappointments
   g) Minimize downtime
   h) Fulfill lawful and administrative prerequisites for information trustworthiness/classification and buyer protection.

6.4 Orientation

Web based business is characterized as the purchasing and offering of items or administrations over electronic frameworks, for example, the Internet and to a lesser degree, other PC systems. It is by and large viewed as the deals and business capacity of e-Business. There has been a monstrous increment in the level of exchange directed electronically since the boundless infiltration of the Internet. A wide assortment of business is led by means of web based business, including electronic assets exchange, production network administration, Internet promoting, online exchange handling, electronic information trade (EDI), stock administration frameworks, and mechanized information gathering frameworks. This monstrous increment in the take-up of web based business has prompted another era of related security dangers, yet any online business framework must meet four indispensable necessities:

a) **Privacy** – data traded must be kept from unapproved parties,

b) **Integrity** – the traded data must not be modified or messed with,

c) **Authentication** – both sender and beneficiary must demonstrate their characters to each other and,

d) **Non-disavowal** – confirmation is required that the traded data was in fact gotten.

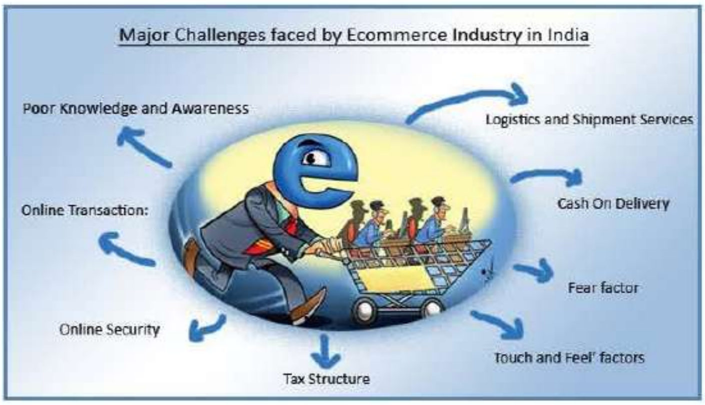

Major Challenges faced by Ecommerce Industry in India
Poor Knowledge and Awareness
Logistics and Shipment Services
Online Transaction:
Cash On Delivery
Fear factor
Online Security
Tax Structure
Touch and Feel' factors

Figure 6.3 Introduction of E-Commerce

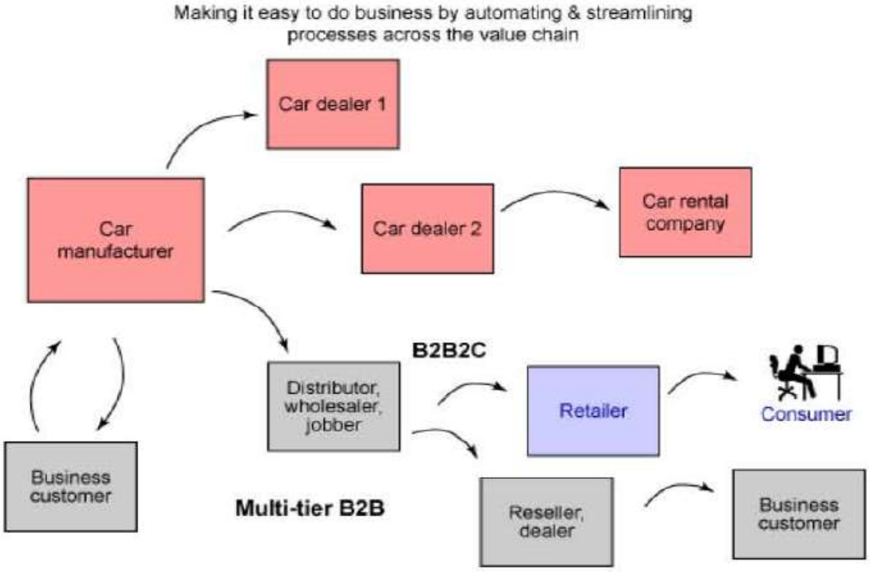


Figure 6.4: Example of online purchasing architecture of E-Commerce

6.5 Client-Server Network

6.5.1 24x7 Accessibility

With a distributed system, if a client needs to get to a document dwelling on another PC, that PC should be fueled on. This is not down to earth with customer gadgets that are for the most part controlled off when not being used. With a customer server arrange, the server is dependably on, constantly accessible, so documents and applications can be gotten to at whatever time.

6.5.2 Centralized, Client Backups

Servers can be arranged to consequently reinforcement customer PCs and furthermore reestablish information in view of those reinforcement pictures, on account of a customer hard drive disappointment.

6.5.3 Remote Access

Servers reinforce remote get to which engages specialists, associates, and customers, to get to data on the server without physically being before the structure.

6.5.4 Server Backups

Intel Xeon-based servers bolster Intel Rapid Storage Technology, which empowers the server to flawlessly store various duplicates of its information on extra inward hard drives, so in the event that one of its hard drives falls flat, it can rapidly recoup the information with insignificant framework downtime.

6.5.5 Improved Collaboration

The server in a customer server system can go about as an incorporated center point for putting away and sharing documents. This arrangement enables different clients to get to documents and rolls out improvements to a solitary brought together duplicate. This likewise limits adaptation control issues that frequently emerge from dealing with different renditions of a similar document.

6.5.6 Enhanced Security

In a client/server environment, each computer still holds (or can still hold) its (or some) resources and files. Other computers can also access the resources stored in a computer, as in a peer-to-peer scenario. One of the particularities of a client/server network is that the files and resources are centralized. This means that a computer, the server, can hold them and other computers can access them. Since the server is always ON, the client machines can access the files and resources without caring whether a certain computer is ON.One of the consequences of a client/server network is that, if the server is turned OFF, its resources and sometimes most of the resources on the network are not available. In fact, one way to set up a client/server network is to have more than one server. In this case, each server can play a different role.Another big advantage of a client/server network is that security is created, managed, and can highly get enforced. To access the network, a person, called a user must provide some credentials, such as a username and a password. If the credentials are not valid, the user is prevented from accessing the network.

6.5.7 Better Client Performance

In a distributed system, customers likewise need to go about as servers, "serving up" administrations to different customers on the system. This can adversely affect execution of those customers. This computational weight is lifted by having a superior, Intel Xeon-based server, dedicated to supporting the clients.

6.5.8 Shared System -Wide Sevices

Servers give shared, brought together administrations for customers to get to, for example ,record ,print, email, database and web facilitating.

6.5.9 Enhanced Reliability

Intel Xeon-based servers bolster Error Correcting Code (ECC) memory which secures your business-basic information and avoid framework blunders via consequently distinguishing and revising memory mistakes.

6.5.10 Business Growth

Distributed systems are constrained as far as the quantity of clients. A customer Server arranges worked with an Intel Xeon based serve r is adaptable for your requirements, permitting space for development as you business develops.

6.6 Emerging Client Server Security Threats

1. **Software Agents and Malicious Code Threats:** The significant danger to security for running customer programming comes about due to the way of the web, customers programs translate information downloaded from self-assertive server from the web. Without beware of imported information, the potential exists for this information to subvert programs running on the frameworks. The security danger emerges when the downloaded information goes through neighborhood mediators, (for example, PostScript) on the customer framework without the client's learning. A littler issue existed in the UNIX mail framework where by a remote client, through different escape arrangements, could summon the shell program (csh or sh) on the beneficiaries machines. This potential security break has been connected to the majority of the new mail framework. In short Client risk for the most part emerges from malevolent information or code. Noxious code alludes to infections, worms, Trojan hoses, sensible bombs and other freak programming programs. Malevolent code is in some cases erroneously connected just with independent PCs however can likewise assault PC arranges effortlessly. In the last case, genuine costs ascribed to the nearness of noxious expenses have come about essentially from framework blackouts and staff times to repair the framework. In any case these expenses can be huge. Customers must sweep for noxious information and executable program parts that are exchanged from the server to the customers. It is possible that the customer may need to filter through information and projects known to be hazardous.

6.7 Threats to Servers

It comprises of pantomime, overhang dropping, foreswearing of administration, bundle replay and parcel alteration. Programmers can utilize electronic listening in to trap client name and decoded passwords sent over the system. They can screen the movement on a framework persistently and imitate a client when the pantomime assault is less inclined to be identified. Encryption can keep spies from acquiring information going over unsecured system. Foreswearing of administration dangers can likewise assaults servers, where a client can render the framework un-usable for true blue clients by embracing an asset or by harming assets so they can't be utilized. The two regular dental of administration assault are administration over-burdening and message flooding. Other complex dangers like bundle replay and adjustment are harder to prepare for. Bundle replay alludes to the recording and retransmission of message parcels in the systems.

a) **Unauthorized Access**- It suggests prohibited access to information, frameworks or applications for some malignant reason. In Passive unapproved get to the programmer tunes in to correspondence channels for discovering insider facts or substance which might be utilized for harming purposes. Notwithstanding, in Active unapproved get to the programmer alters framework or information with a goal to control or change. Some present cases incorporate incapable encryption or absence of encryption for home remote systems, a prevalent home-saving money framework that stores a client's record number in a Web "treat" which threatening sites can split and mail-borne infections that can take the client's monetary information from the neighborhood circle or even from the client's keystrokes. Home PC, Point-of-Sale (POS) terminals in physical stores, and additionally an assortment of versatile and handheld gadgets can without much of a stretch is focused by programmers.

b) **Denial of Service**- It may occur by spamming and viruses. Spamming is basically unusual e-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. DDOS (Distributed Denial Of service Attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. However, viruses are self-replicating computer programs designed to perform unwanted events. Worms are special viruses that spread using direct Internet connections and Trojan Horses are disguised as legitimate software that trick users into running the program.

c) **Theft and Fraud**- Extortion happens when the stolen information is utilized or altered. Robbery of programming suggests unlawful replicating from organization's servers or burglary of equipment, particularly portable

PCs. Programmers break into uncertain trader web servers to reap documents of MasterCard numbers by and large put away alongside individual data when a customer makes an online buy. The vendor back-end and database is additionally defenseless for robbery from outsider satisfaction focuses and other preparing operators.

6.8 Protecting the Environment

The worldwide spread of Internet makes positive conditions for the development of electronic trade. In the meantime, this is a test to the lawful system of numerous nations on the grounds that the lawful structure is inadequately adaptable or deficiently particular in directing the new relations between business substances. The Internet business introduces the accompanying issues to the lawful system of states:

6.8.1 Distance Transactions

More regularly than any time in recent memory the purchaser vender relations are losing direct contact. On the Internet it might happen that neither one of the parties to the exchange thinks about the exchange until it is expected to be performed, not to mention have the composed type of the exchange. New conditions and structures for the authority of exchanges are fundamental. It is likewise basic to have implies how to characterize the obligation of the gatherings.

6.8.2 Payments

New installment strategies and means have developed in people in general condition of the wide world web. Practically every exchange of this kind includes, notwithstanding the purchaser or vender, their banks and the administrators of the installment frameworks, assuming any. Since the quantity of fakes using electronic installment means is very significant nowadays, the obligation of each gathering must be unambiguously characterized.

6.8.3 International aspects

Even though electronic trade does not perceive national outskirts, they are as yet perceived by business law. The current particular lawful acts, tax assessment guidelines and limitations on imports sends out still remain a vital, ease back moving issue to legal advisors.

6.8.4 Consumer Protection

The populace requires ensures that the introduction of merchandise and enterprises on the Internet ought to adjust to their qualities that the purchaser ought to be qualified for give back the procured faulty item that the shopper ought to be secured against undesired publicizing or against the uncalled for utilization of his/her own information.

6.8.5 Protection of Trademarks, Internet and Intellectual Property

The region bound character of law identified with these types of property runs counter to the substances of the cross-outskirt nature of the Internet, while the computerized type of numerous items disseminated in the internet is particularly helpless against illicit duplicating.

6.8.6 Directive on Distance Transactions

The Directive on Distance Transactions, embraced in 1997, manages the standards of shopper assurance in regard of exchanges reached of the gatherings: by phone, post, electronic means. The primary arrangements of the Directive are the accompanying:

a) **Confirmation of the transaction:** After the terminate of the exchange, the shopper ought to get an affirmation in the medium adequate to both sides (e. g. by email or on paper).

b) **Right of revocation:** The shopper is qualified for pull back from the exchange inside 7 business days with no punishment or necessity to create reasons.

c) **Full information:** The merchant must advise the purchaser in advance of the correct costs for the merchandise and ventures offered (and additionally whatever other charges), their legitimacy date, conveyance costs and their exact qualities.

d) **Prohibition on inert transactions:** Exchanges which are not authorized by the buyer are restricted regardless of the possibility that the shopper has been educated of the ways how he may pull back from the exchange.

6.8.7 Directive on Electronic Commerce

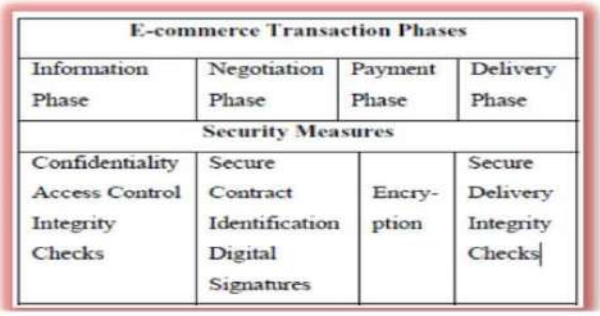
This most recent lawful act exceptionally intended for advanced business sets down, in addition to other things, the necessities for the supplier of data society administrations (ISS) and the administrative standards of his business:

a) **Identification:** The gatherings must guarantee that data on the ISS providers, set up on their domain, name, postal and email locations, enrollment and VAT code ought to be effortlessly open to buyers and skillful foundations.

b) **Commercial correspondence.** In the event that the IVP comprises, to some degree or in entire, of material of publicizing nature, the specialist organization must distinguish it expressly accordingly and demonstrate the characteristic individual or lawful substance spoken to by it. The same is pertinent to refunds, recreations, unique offers, endowments, and so on. The Directive requires that part states ought to control the unapproved wellsprings of business correspondence appropriated by means of email inside their legitimate system.

c) **Electronic Transactions:** Part States must guarantee that their laws ought to accommodate the legitimacy of electronic business exchanges. The specialist co-op must advise, obviously and unambiguously, the administration beneficiary of all the specialized strides important to make the exchange. After the finish of the exchange the specialist co-op must issue the affirmation/receipt of the exchange. All through this procedure, up to the last stage, the beneficiary of the administration must have the likelihood of pulling back from the exchange or right any missteps.

d) **The responsibility of the communications intermediary:** Electronic communications intermediaries, i.e. the suppliers of administrations of Internet interchanges and media communications administrators, are not in charge of the substance transmitted or put by utilizing their administrations or for the exchanges made. The electronic correspondences middle people are not obliged to screen the transmitted or spared data for conceivable unlawful exercises.



E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry- ption	Secure Delivery Integrity Checks

Figure 6.5: Transactions and security measures for E-Commerce

6.8.8 Mandate on the Harmonization of Copyright and Related Rights in the Data Society (Draft)

The endless potential outcomes for the dissemination of music and video deals with the Internet have been hampered by the similarly unfathomable advanced pilfering wave. This archive, which is under consideration in the European Parliament, meets the necessity of the diversion business to ensure copyright and the security of advancements used to guarantee the copyright. Notwithstanding, the mandate still allows to make duplicates solely for individual utilize, however just by simple innovation (i.e. duplicating from a CD to MP3 would be illicit). Moreover, illicit are projects and means intended to "break" the counter privateer security.

6.8.9 The Law on Electronic Signature

The main successful authoritative report particularly intended for electronic information correspondences is the Law on Electronic Signature, embraced in 2000. The electronic mark is an uncommon supplement, shaped by a cryptographic calculation, to an advanced archive. It is indistinguishable from the substance of the report and the electronic endorsement of its creator. The reason for the electronic signature, similarly as that of an ordinary mark, is to guarantee the validness of the report's creator and substance. The beneficiary of the report utilizes another calculation which thinks about the advanced mark to the archive and its creator's open declaration. This calculation perceives if the content of the archive has been adjusted without utilizing the first declaration.

6.9 Trust-Based Security

Technologies used for e-commerce Security:

a) Encryption calculations like Public Key Infrastructure (PKI) frameworks which depend on unbalanced cryptography are exceptionally secure as they are combined with Secure Socket Layer (SSL) convention and the interbank standard suite, ANSI X9. PKI frequently requires a brought together, profoundly accessible go-between for key administration, and particularly for incite notice about renounced key-sets.

b) A computerized signature, which can be utilized to sign contracts, to demonstrate personality for get to or to give credibility of an electronic dissemination is the best case of PKI.

c) Smartcards can be utilized to store information about the carrier of the card, including distinguishing proof qualifications, money related information, therapeutic records and so on. Smartcards can enable POS exchanges to be more multifaceted, in light of the fact that the whole client's information is constantly accessible. This design can likewise stay away from the brought together capacity of by and by delicate information.

d) Digital money and organized installments through which a shopper may purchase electronic information or an advanced administration without uncovering his buys to a budgetary clearinghouse and personality to the dealer. Micropayments, for example, per-article daily paper memberships and PayPal, an installment delegate, have additionally been monetarily effective.

e) Digital watermarking innovation is another well known web security instrument where the specialized objective is to discover methods for cryptographically labeling electronic substance (particularly pictures and sound) in a way that is non removable, non-forgeable, and unmistakable. The watermark tag is for the most part intended to be undetectable or inconspicuous.

Trust is an imperative issue in web based business, on the grounds that not at all like genuine exchanges, the retailer is absent face to face amid the exchange and the customer is not managing a genuine individual. It is simply managing an interface. It is substantially simpler for an element to set up a site and an electronic installment handling framework than a true retail facade. It is less expensive, speedier and more straightforward. It is likewise substantially more troublesome for clients to decide the legitimacy of sites. This makes it extremely hard to trust that the retailers are who they claim to be. Trust is a mental alternate route that customers can utilize when attempting to diminish the instability and many-sided quality of exchanges and connections in web based business markets. Online it is hard to associate characters with genuine people. For customers, security, protection, usefulness and ease of use issues are thought to be hindrances to internet shopping.

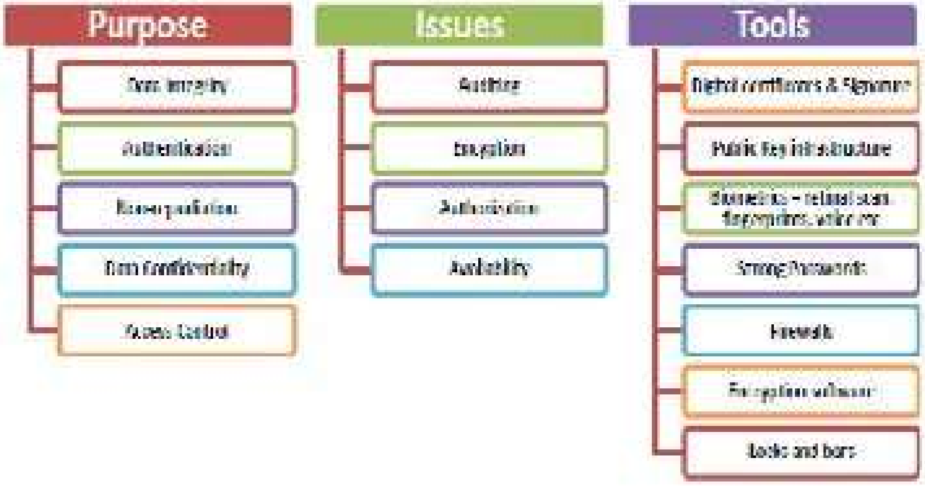


Figure 6.6: Various Purposes, Issues and Tools useful in E-Commerce

Additionally, they need their own information to be private and classified with the goal that they are not presented to any extortion. They additionally need that the innovation they are utilizing ought to empower them to openly work and take sensible control over it. Be that as it may, they are more adaptable and willing towards going for broke with the general population or associations that they trust. The plausible hazard is higher in internet business fundamentally in light of ignorance, vicinity and irrelevant physical communications. In this way, to perceive any reason why purchaser draw in or don't take part in web based business, it is vital to concentrate their online trust in web based business as a commercial center.

6.10 Security through Obscurity (STO)

Security through lack of definition (STO) is dependence upon mystery in programming improvement to limit the possibility that shortcomings might be identified and focused on. Security through indefinite quality is frequently accomplished by creating code in mystery, shielding it from unapproved get to and keeping up the product's restrictive shut source status. The approach can be powerful in mix with different measures yet STO all alone is expostulated. Used to reinforce more powerful methodologies, for example, security by outline, security through lack of definition can include another layer of assurance.

Security through minority is a subcategory of STO that depends on code that is occasionally utilized. That approach depends on the information that programmers searching for vulnerabilities to abuse regularly look for normally utilized programming to boost offers of malware and hacking scripts and increment the quantity of PCs they can reach. Correspondingly, security through outdated nature depends on the way that projects that are no longer utilized are less inclined to be misused on the grounds that few know about coding for them- - not to mention abusing their code. Security through differing qualities can likewise be compelling. This approach includes utilizing a blend of piecemeal segments. Security through assorted qualities can make a framework harder to target and can be naturally more secure than an outstanding solid arrangement.

6.11 Password Schemes

This security arrangement erects a first level hindrance to unintentional interruption. In fact, in any case, secret word plans do minimal about think assault, uniquely, when normal words or legitimate names are chosen as passwords. Having unmistakable passwords for a particular gadget is fairly issue, since will record them, share them or incorporate them in programmed script. To counter these dangers different methodologies have been recommended for making one time passwords, including savvy cards, randomized tokens and test reaction plans.

Encryption and Decryption: Encryption is the way toward changing data so it is muddled to anybody however the expected beneficiary. Decoding is the way toward changing scrambled data so it is understandable once more. A cryptographic calculation, additionally called a figure, is a numerical capacity utilized for encryption or unscrambling. By and large, two related capacities are utilized, one for encryption and the other for decoding. With most present day cryptography, the capacity to keep encoded data mystery is constructing not in light of the cryptography calculation, which is generally known, however on a number called a key that must be utilized with the calculation to deliver a scrambled outcome or to decode beforehand scrambled data. The utilized of keys for encryption and unscrambling.

a) Symmetric-Key Encryption: With symmetric-key encryption, the encryption key can be ascertained from the unscrambling key and the other way around. With most symmetric calculations, a similar key is utilized for both encryption and unscrambling.

b) Public-Key Encryption: It includes a couple of keys and a private key-related with a substance that requirements to confirm its character electronically or to sign or scrambles information. Every open key is distributed and the relating private key is kept mystery. Information encoded with your open key can be unscrambled just with your private key.

c) Key Length and Encryption Strength: Encryption quality is frequently portrayed regarding the measure of the keys used to play out the encryption; by and large, longer keys give more grounded encryption. Enter length is measured in bits. For instance, 128-bits keys for use with the CR4 symmetric key figure bolstered by SSL (Secure Socket Layer) give fundamentally preferable cryptographic insurance over 40-bit keys for use with a similar

figure.

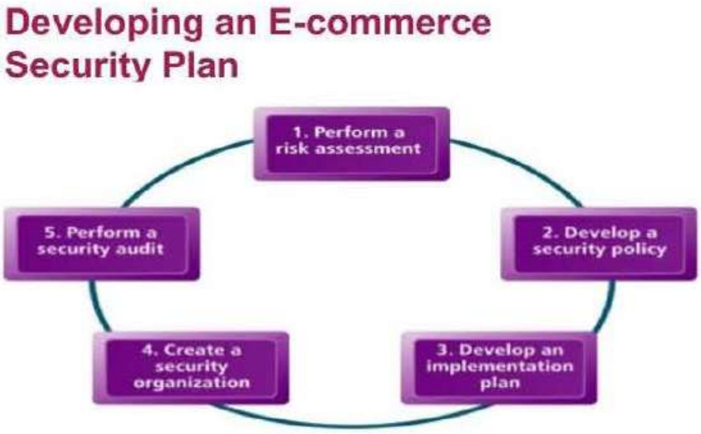

Developing an E-commerce Security Plan
1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

Figure 6.7: Development of Security plan of E-Commerce

Encrypted documents & Emails: Email client would covet privacy and sender confirmations are utilizing encryption. Encryption is basically proposed to keep individual considerations individual. Email is regularly encoded for the reason that all system correspondence is open for listening in. Web email is clearly far-less secure than the postal framework, where conceals shields correspondence from easygoing snooping. A look at the header territory of any email message by complexity, will demonstrate that it has gone through various hubs on its approach to you. Each one of these hubs shows the open door for snooping. Regular correspondence over telephone and fax line involves security dangers. Regardless of jumps in innovation and wide uses, fax transmission is not yet broadly scrambled. The principle reason is the bother of preparing both the sending and accepting machines with good encryption before copy transmission. Email programming is progressively consolidating particular choices that disentangle encryption and decoding. Examination of encoded data is non-unimportant; each record must be unscrambled even before it can be inspected.

Email Encryption Schemes Deployed On Internet:

a) **Privacy enhanced mail standard (PEM):** It is planned purposed however not yet authoritatively received by the web exercises board to give secure email over the web. Configuration to work with current web messages groups, PEM incorporates encryption verification and key administration, and permits utilization of both open key and mystery key cryptosystems. PEM expressly underpins just a couple of cryptographic calculations; other might be included later. It additionally gives backings to non-renouncement, which permits the outsider beneficiary of a sent message to confirm the character of the message originator and to check whether any of the first content has been adjusted.

b) **Pretty Good Privacy (PGP):** It is a usage of open key cryptography in view of RSA. It is a free programming bundle that scrambles email. PGP is broadly utilized, and its development is being powered by the fast development in web utilize and the expanding dependence on email for everything from authoritative reports to any letter. It gives secure encryption of reports and information records that even propelled super PCs are unable to "break". PGP gives secretly by encoding message to be transmitted or to be put away locally as records. In both cases, the regular encryptions calculation known as IDEA (International Data Encryption Algorithm) is utilized. Any mystery key encryption framework must address the issue of key dispersion; in PGP each key is utilized just ones i.e. another key is produced as an arbitrary number for each message. Many individuals routinely incorporate their PGP unique mark in email message.

c) **Client Server Network Security**: It is one of the greatest cerebral pains framework manager confront as they adjust the restricting objective of client mobility and simple get to and site security and privacy of nearby data. Arrange security on the web is a noteworthy worry for business associations, particularly beat administration. As of late the web has raised numerous new security concerns. By interfacing with the web, a neighborhood arranges association might open itself to the whole populace on the web. A web association viably ruptures physical security border of the corporate system and opens itself to access from other system containing people in general web. That being the situation, the trough of even the most casual association must give careful consideration to security. For much business operation, security will just involve ensuring that current framework elements, for example, secret word and benefits, are limited appropriately. They have to review all entrance to the system. A framework that records all sign on endeavors especially the unsuccessful ones-can modify director to the requirement for more grounded measures. However where privileged insights are in question or were imperative corporate resources must be made accessible to remote clients, extra measures must be taken. Programmers can utilize watchword speculating, secret key catching, security openings in projects, or normal system get to strategies to imitate clients and in this way represent a risk to the server.

Client Server Network Security Problem Manifest Themselves In 3 Ways:

a) **Physical security holes**: It comes about when individual increases unapproved physical access to the PC. A decent e.g. would be an open workstation room, where it would be simple for a meandering programmer to reboot a machine into single client mode and temper with the records, if safety measures are not taken. On the system this is likewise a typical issue, as programmers access arrange framework by speculating passwords of different clients.

b) **Software Security holes:** It comes about when gravely composed program or "favored" programming is "bargained" into doing things they shouldn't. The most renowned e.g. of this is the "send letters" gap, which pushed the web to the brink of collapse in 1988. A later issue was the (a vindictive programmers) to make a "root" shell or super client get to mode. This is the most abnormal amount of get to conceivable and could be utilized to erase the whole document framework or make new record or secret word document bringing about in-measurable harm.

c) **Inconsistent uses holes:** It comes about when framework overseer collects blend of equipment and programming with the end goal that the framework is genuinely defective from a security perspective. The inconsistency of endeavoring 2 detached yet helpful things makes the security openings. Issues like this are hard to disengage ones a framework is setup and running so it is ideal to painstakingly manufacture the framework in light of them. This sort of issue is getting to be noticeably basic as programming turns out to be more minds boggling.

6.12 Biometric Systems

It is the most secure level of approval, include some extraordinary parts of a man's body. It is exceptionally costly to execute at a cost. A biometric framework is a mechanical framework that utilizations data about a man (or other natural living being) to recognize that individual. Biometric frameworks depend on particular information about remarkable natural characteristics with a specific end goal to work adequately. They might be more qualified for controlling physical get to – where one biometric unit can serve for some specialist then for system or workstation get to. Past biometric confirmation depended on examination of fingerprints, palm prints, retinal examples or on mark check or voice acknowledgment.

Seven elements to be utilized while surveying the reasonableness of any quality for use in biometric validation demonstrated as follows:

- Universality implies that each individual utilizing a framework ought to have the quality.
- Uniqueness implies the quality ought to be adequately unique for people in the important populace to such an extent that they can be recognized from each other.
- Permanence identifies with the way in which an attribute changes after some time. All the more particularly, a quality with "great" changelessness

will be sensibly invariant after some time regarding the particular coordinating calculation.

- Measurability (collectability) identifies with the simplicity of securing or estimation of the attribute. Furthermore, procured information ought to be in a frame that licenses resulting preparing and extraction of the applicable capabilities.
- Performance identifies with the exactness, speed, and strength of innovation utilized (see execution segment for more subtle elements).
- Acceptability identifies with how well people in the pertinent populace acknowledge the innovation to such an extent that they will have their biometric attribute caught and surveyed.
- Circumvention identifies with the straightforwardness with which a characteristic may be imitated utilizing an antiquity or substitute.

Figure 6.8: Biometric Systems for palm and finger print functionality

6.13 Self Learning Exercise

Q.1 Encryption can be done

a) only on textual data

b) only on ASCII coded data

c) on any bit string

d) only on mnemonic data

Q.2 A digital signature is

a) Scanned signature

b) signature in binary form

c) Encrypting information

d) handwritten signature

Q.3 Mechanism to protect private networks from outside attack is

a) Firewall

b) 0Antivirus

c) Digital signature

d) Formatting

Q.4 EDI standard

a) is not easily available

b) defines several hundred transaction sets for various business forms

c) is not popular

d) defines only a transmission protocol

Q.5 What encourages users of a product or service supplied by a B2C company to ask friends to join in as well?

a) Spam

b) Viral marketing

c) Affiliate programs

d) None of the above

Q.6 Secret-key encryption is also known as

a) Asymmetric encryption

b) Symmetric encryption

c) Secret-encryption

d) Private encryption

Q.7 All of the following are techniques B2C e-commerce companies use to attract customers, except

a) Registering with search engines

b) Viral marketing

c) Online Ads

d) Virtual marketing

Q.8 A hashing function for digital signature

i) must give a hashed message which is shorter than the original message

ii) must be hardware implementable

iii) two different messages should not give the same hashed message

iv) is not essential for implementing digital signature

a) i and ii

b) ii and iii

c) i and iii

d) iii and iv

6.14 Summery

Security issues turn out to be more mind boggling in a system situation. We should guarantee that entrance to the system is controlled and that information is not powerless against assault amid transmission over the system. A security hazard is characterized as a situation, condition or occasion with the possibility to make monetary hardship information or system assets as devastation, change of information, disavowal of administration or extortion, waste and manhandle. Customer server security utilizes different approval techniques to ensure that lone legitimate client and projects have entry to data assets, for example, database. Information and exchange security guarantee the protection and privately in electronic message and information bundles, including the confirmation of remote clients in the system exchanges for exercises, for example, on line installments.

The goals are to defeat any attempt to expect another identity while included with electronic mail or distinctive sorts of data correspondence. Preventive measures join data encryption using diverse cryptographic strategies.

Web based business security is the insurance of internet business resources from unapproved get to, utilize, modification, or annihilation.

Six measurements of internet business security:

1. **Respectability:** counteractive action against unapproved information adjustment.
2. **Non-revocation:** counteractive action against any one gathering from reneging on an understanding afterward.
3. **Genuineness:** validation of information source.
4. **Classification**: assurance against unapproved information divulgence.
5. **Protection:** arrangement of information control and revelation.

6. **Accessibility:** counteractive action against information deferrals or expulsion.

6.15 Glossary

Web based business THREATS: Threats can be anybody with the capacity, innovation, opportunity, and expectation to do hurt. Potential dangers can be remote or local, inside or outside, state-supported or a solitary maverick component. Fear based oppressors, insiders, disappointed workers, and programmers are incorporated into this profile (President's Commission on Critical Infrastructure Protection).

1. Licensed innovation dangers - utilize existing materials found on the Internet without the proprietor's authorization, e.g., music downloading, space name (digital crouching), programming pilfering
2. Customer PC dangers
   - Malicious codes
   - Active substance
3. Correspondence channel dangers
   - Sniffer program
   - Backdoor
   - Spoofing
   - Denial-of-administration
4. Server dangers
   - Privilege setting
   - Server Side Include (SSI), Common Gateway Interface (CGI)
   - File exchange
   - Spamming

6.16 Answers to Self Learning Exercise

Q.1 (c)

Q.2 (d)

Q.3 (a)

Q.4 (b)

Q.5 (b)

Q.6 (d)

Q.7 (d)

Q.8 (d)

Q.9 (c)

6.17 Exercise

Q.1 What is E-commerce? Explain advantages and disadvantages of E-Commerce.

Q.2 Explain the security issues of E-Commerce.

Q.3 Explain the threats components of E-Commerce.

Q.4 Explain different protection schemes of E-Commerce.

Q.5 What are the different security models of E-Commerce for privacy?

Q.6 Explain about privacy issues through e- purchasing?

Q.7 Explain about the electronic signature in E-commerce?

Q.8 What is e-commerce security and why is it important?

Q.9 How to identify threats to e-commerce?

Q.10 How to determine ways to protect e-commerce from those threats?

Q.11 What are electronic payment systems?

Q.12 What are the security requirements for electronic payment systems?

Q.13 What security measures are used to meet these requirements?

References and Suggested Readings

1. Security fundamentals for E-Commerce by Vesna Hassler, Arctic House.
2. E-commerce Agents by jimingx Liu and Yiming by Springer.
3. Essentials of Online Payment Security and Fraud Prevention by David Montahue.
4. E-Commerce Security and Privacy (Advances in Information Security), by Anup K. Ghosh.

UNIT-7

Threats and Security

Structure of the Unit

7.0 Objective

In this unit we shall learn the following topics

- Software Agents and Malicious code Threat
- Trojan horses, Malwares, Worms, Viruses
- Introductory cryptography

7.1 Introduction

A circulated foreswearing of-administration (DDoS) assault — or DDoS assault — is the point at which a vindictive client gets a system of zombie PCs to disrupt a particular site or server. The assault happens when the malevolent client advises the entire zombie PCs to contact a particular site or server again and again. That expansion in the volume of activity over-burdens the site or server making it is moderate for true blue clients, here and there to the point that the site or server closes down totally. By exploiting security vulnerabilities or shortcomings, an aggressor could take control of your PC. The most well-known and clear kind of DDoS assault happens when an aggressor "surges" a system with futile data. When you write a URL into your program, you are sending a demand to that site's PC server to see the page. The server can just process a specific number of solicitations without a moment's delay. On the off chance that an aggressor over-burdens the server with solicitations, it can't prepare yours. The surge of approaching messages to the objective framework basically compels it to close down, in this way denying access to real clients.

Figure 7.1 : Cyber Attack and Data Breach for Security

PCs and systems initially were worked to facilitate the trading of data. Early data innovation (IT) foundations were worked around focal PCs or centralized server arrangements while others were produced around the PC. What some idea inconceivable progressed toward becoming reality and today organizations are being driven by the energy of the PC that clients access with only a client name and watchword. Be that as it may, as the data upheaval opened new roads for IT, it additionally opened new potential outcomes for wrongdoing. Assailants utilized these chances to take passwords and access data or to make awful consequences for systems and PCs.

Figure 7.2: computer-protection-from-threats is needed

The server can just process a specific number of solicitations without a moment's delay. In the event that an assailant over-burdens the server with solicitations, it can't prepare yours. The surge of approaching messages to the objective framework basically constrains it to close down, in this way denying access to honest to goodness clients.

7.2 History

The best risk to PC frameworks and their data originates from people, through activities that are either noxious or uninformed. At the point when the activity is pernicious, some inspiration or objective is by and large behind the assault. For example, the objective could be to disturb typical business operations, along these lines denying information accessibility and creation. This could occur between two opponent organizations or even as a scam. To accomplish their objectives, aggressors utilize surely understood procedures and strategies to endeavour vulnerabilities in security approaches and frameworks. The following segment on security manages the general dangers related with PC frameworks and talks about the thought processes or objectives the aggressors have procedures and techniques for getting entrance, and the different vulnerabilities that could exist in frameworks and security arrangements.

7.3 Overview

Data is the key resource in many associations. Organizations pick up an upper hand by knowing how to utilize that data. The risk originates from other people who might want to obtain the data or point of confinement business openings by meddling with typical business forms. The question of security is to ensure profitable or touchy hierarchical data while making it promptly accessible. Aggressors attempting to hurt a framework or upset typical business operations misuse vulnerabilities by utilizing different strategies, techniques, and instruments. Framework chairmen need to comprehend the different parts of security to create measures and approaches to ensure resources and utmost their vulnerabilities. Assailants for the most part have intentions or objectives—for instance, to upset ordinary business operations or take data. To accomplish these intentions or objectives, they utilize different strategies, apparatuses, and procedures to endeavour vulnerabilities in a PC framework or security approach and controls.

7.4 Orientation

1) The Need for Security: Administrators regularly find that assembling a security arrangement that confines both clients and assaults is tedious and exorbitant. Clients likewise end up noticeably displeased at the overwhelming security strategies making their work troublesome for no discernable reason, bringing on terrible governmental issues inside the organization. Arranging a review approach on gigantic systems takes up both server assets and time, and frequently chairmen take no note of the inspected occasions. A typical disposition among clients is that if no mystery work is being performed, why try executing security. There is a cost to pay when a weak security plan is put without hesitation. It can bring about surprising fiasco. A secret key arrangement that enables clients to utilize clear or feeble passwords is a programmer's heaven. No firewall or intermediary assurance between the association's private neighbourhood (LAN) and people in general Internet makes the organization an objective for digital wrongdoing. Associations should decide the value they will pay keeping in mind the end goal to secure information and different resources.

This cost must be weighed against the expenses of losing data and equipment and upsetting administrations. The thought is to locate the right adjust. On the off chance that the information needs negligible security and the loss of that information is not going to cost the organization, then the cost of ensuring that information will be less. On the off chance that the information is delicate and needs greatest assurance, then the inverse is typically valid.

2) Dangers: In PC security a risk is a conceivable peril that may abuse a powerlessness to break security and in this manner cause conceivable mischief. A danger can be either "purposeful" (i.e. hacking: an individual saltine or a criminal association) or "unintentional" (e.g. the likelihood of a PC breaking down, or the likelihood of a catastrophic event, for example, a seismic tremor, a fire, or a tornado) or generally a condition, ability, activity, or occasion. An asset (both physical and coherent) can have at least one vulnerabilities that can be abused by a risk specialist in a danger activity. The outcome can possibly trade off the secrecy, uprightness or accessibility properties of assets (conceivably unique in relation to the defenceless one) of the association and others included gatherings (clients, providers). Dangers can be ordered by their sort and source.Types of threats:
   a. Physical damage: fire, water, pollution
   b. Natural events: climatic, seismic, volcanic
   c. Loss of essential services: electrical power, air conditioning, telecommunication
   d. Compromise of information: eavesdropping, theft of media, retrieval of discarded materials
   e. Technical failures: equipment, software, capacity saturation,
   f. Compromise of functions: error in use, abuse of rights, denial of actions
3) A threat type can have multiple origins.
4) Deliberate: aiming at information asset
   a. spying
   b. illegal processing of data
5) Accidental

    a. equipment failure
    b. software failure

6) Environmental
    a. natural event
    b. loss of power supply

7) Negligence: Known but neglected factors, compromising the network safety and sustainability

7.5 Software Agents and Malicious Code Threat

PC security risks are consistently imaginative. Supervisors of cover and control, these perils persistently create to find better ways to deal with annoy, take and devilishness. Arm yourself with information and resources for shield against flighty and creating PC security perils and stay safe on the web.

Computer Virus Threats: Maybe the most surely understood PC security danger, a PC infection is a program written to modify the way a PC works, without the consent or learning of the client. An infection repeats and executes itself, for the most part doing harm to your PC simultaneously. Figure out how to battle PC infection dangers and remain safe on the web.

Spyware Threats: A genuine PC security danger, spyware is any program that screens your online exercises or introduces programs without your assent for benefit or to catch individual data. We've amassed an abundance of information that will help you battle spyware dangers and remain safe on the web.

Hackers & Predators: Individuals, not PCs, make PC security dangers and malware. Programmers and predators are software engineers who defraud others for their own pick up by breaking into PC frameworks to take, change or pulverize data as a type of digital fear mongering.

Phishing Threats: Taking on the appearance of a dependable individual or business, phishes endeavor to take delicate budgetary or individual data through fake email or texts. How might you differentiate between a genuine message and a phishing trick? Instruct yourself on the most recent traps and tricks.

7.6 Trojan Horses

A Trojan steed is vindictive code that, notwithstanding its essential impact, has a moment, no undeniable malevolent impact. For instance of a PC Trojan steed, a rationale bomb is a class of malevolent code that "explodes" or goes off when a predefined condition happens. A period bomb is a rationale bomb whose trigger is a period or date. A trapdoor or secondary passage is a component in a program by which somebody can get to the program other than by the self-evident, coordinate call, maybe with unique benefits. For example, a computerized bank employee program may permit anybody entering the number 990099 on the keypad to handle the log of everybody's exchanges at that machine. In this illustration, the trapdoor could be deliberate, for upkeep purposes, or it could be an illegal route for the implementer to wipe out any record of a wrongdoing.

7.7 Malwares

Malware, short for vindictive programming, is any product used to disturb PC or portable operations, assemble touchy data, access private PC frameworks, or show undesirable promoting. The main classification of malware proliferation concerns parasitic programming sections that connect themselves to some current executable substance. The section might be machine code that contaminates some current application, utility, or framework program, or even the code used to boot a PC framework. Malware is characterized by its malevolent aim, acting against the necessities of the PC client, and does exclude programming that causes accidental mischief because of some inadequacy. Malware might be stealthy, proposed to take data or keep an eye on PC clients for a developed period without their insight, as Reign, or it might be intended to bring about mischief, regularly as harm, or to coerce instalment (Crypto Locker).

"Malware" is an umbrella term used to allude to an assortment of types of antagonistic or meddlesome programming, including PC infections, worms, and Trojan stallions, recover product, spyware, adware, frighten product, and different vindictive projects. It can appear as executable code, scripts, dynamic substance, and other programming. Spyware or other malware is once in a while discovered implanted in projects provided formally by organizations, e.g., downloadable from sites, that seems helpful or alluring, however may have, for instance, extra concealed following usefulness that assembles promoting measurements. A case of such programming, which was portrayed as ill-conceived, is the Sony root pack, a Trojan implanted into CDs sold by Sony, which noiselessly introduced and disguised itself on buyers' PCs with the aim of forestalling illegal replicating; it additionally given an account of clients' listening propensities, and unexpectedly made vulnerabilities that were misused by inconsequential malware.

7.8 Worms

A PC worm is an independent malware PC program that recreates itself keeping in mind the end goal to spread to different PCs. Regularly, it utilizes a PC system to spread itself, depending on security disappointments on the objective PC to get to it. Worms quite often cause in any event some mischief to the system, regardless of the possibility that exclusive by expending data transmission, though infections quite often degenerate or change records on a focused on PC. Many worms that have been made are planned just to spread, and don't endeavour to change the frameworks they go through. In any case, as the Morris-worm and My-fate appeared, even these "payload free" worms can bring about real interruption by expanding system activity and other unintended impacts. Any code intended to accomplish more than spread the worm is commonly alluded to as the "payload". Commonplace noxious payloads may erase records on a host framework (e.g., the Explore Zip worm), encode documents in a payoff product assault, or elate, for example, classified archives or passwords. Likely the most widely recognized payload for worms is to introduce an indirect access. This enables the PC to be remotely controlled by the worm creator as a "zombie". Systems of such machines are regularly alluded to as botnets and are ordinarily utilized for a scope of pernicious purposes, including sending Spam or performing DoS assaults.

Worms spread by misusing vulnerabilities in working frameworks. Merchants with security issues supply general security refreshes (see "Fix Tuesday"), and if these are introduced to a machine then the greater part of worms can't spread to it. On the off chance that defencelessness is uncovered before the security fix discharged by the seller, a zero-day assault is conceivable. Clients should be careful about opening unforeseen email, and ought not run appended documents or projects, or visit sites that are connected to such messages. Be that as it may, as with the "ILOVEYOU" worm, and with the expanded development and proficiency of phishing assaults, it stays conceivable to trap the end-client into running malignant code. Against infection and hostile to spyware programming are useful, yet should be stayed up with the latest with new example documents no less than each couple of days. The utilization of a firewall is likewise suggested.

7.9 Viruses

A PC infection is a sort of noxious programming program ("malware") that, when executed, recreates by imitating itself (replicating its own particular source code) or tainting other PC programs by altering them. Tainting PC projects can incorporate too, information documents, or the "boot" division of the hard drive. At the point when this replication succeeds, the influenced regions are then said to be "tainted" with a PC infection. The expression "infection" is likewise regularly, however incorrectly, used to allude to different sorts of malware. "Malware" envelops PC infections alongside numerous different types of pernicious programming, for example, PC "worms", ransomware, Trojan stallions, key lumberjacks, root units, spyware, adware, malignant Browser and different noxious programming. The larger part of dynamic malware dangers are really Trojan steed projects or PC worms instead of PC infections. The term PC infection, instituted by Fred Cohen in 1985, is a misnomer. Infections regularly play out some sort of destructive action on contaminated host PCs, for example, securing of hard plate space or focal preparing unit (CPU) time, getting to private data (e.g., Visa numbers), tainting information, showing political or silly messages on the client's screen, spamming their email contacts, logging their keystrokes, or notwithstanding rendering the PC pointless. Nonetheless, not all infections convey a damaging "payload" and endeavor to conceal themselves—the characterizing normal for infections is that they are self-reproducing PC programs which introduce themselves without client assent.

Infection scholars utilize social designing double dealings and endeavor point by point information of security vulnerabilities to access their hosts' PCs and processing assets. By far most of infections target frameworks running Microsoft Windows, utilizing an assortment of systems to taint new has, and frequently utilizing complex against location/stealth techniques to avoid antivirus programming. PC infections presently cause billions of dollars of financial harm every year, because of bringing on framework disappointment, squandering PC assets, adulterating information, expanding support costs, and so forth. Accordingly, free, open-source antivirus instruments have been produced, and an industry of antivirus programming has sprung up, offering or unreservedly appropriating infection insurance to clients of different working frameworks.

Operation and Functions:

Parts: A reasonable PC infection must contain an inquiry schedule, which finds new documents or new plates which are beneficial focuses for disease. Furthermore, every PC infection must contain a routine to duplicate itself into the program which the hunt routine finds. The three primary infection parts are:

Infection Mechanism: Contamination instrument (likewise called 'disease vector'), is the manner by which the infection spreads or proliferates. An infection commonly has an inquiry schedule, which finds new records or new plates for contamination.

Trigger: The trigger, which is otherwise called rationale bomb, is the ordered form that could be enacted at whatever time an executable record with the infection is run that decides the occasion or condition for the vindictive "payload" to be initiated or conveyed, for example, a specific date, a specific time, specific nearness of another program, limit of the plate surpassing some point of confinement, or a double tap that opens a specific document.

Payload: The "payload" is the genuine body or information that play out the real vindictive reason for the infection. Payload action may be perceptible (e.g., on the grounds that it makes the framework back off or "solidify"), as more often than not simply the "payload" is the hurtful action, or at times non-dangerous however distributive, which is called Virus trick.

Dormant Phase: The infection program is sit without moving amid this stage. The infection program has figured out how to get to the objective client's PC or programming, yet amid this stage, the infection does not make any move. The infection will in the end be actuated by the "trigger" which states which occasion will execute the infection, for example, a date, the nearness of another program or record, the limit of the plate surpassing some point of confinement or the client making a specific move (e.g., double tapping on a specific symbol, opening an email, and so on.).

Propagation Phase: The infection begins proliferating, that is duplicating and reproducing itself. The infection puts a duplicate of itself into different projects or into certain framework zones on the circle. The duplicate may not be indistinguishable to the proliferating variant; infections frequently "transform" or change to avoid discovery by IT experts and against infection programming. Each contaminated program will now contain a clone of the infection, which will itself enter a proliferation stage.

Triggering Phase: A lethargic infection moves into this stage when it is enacted, and will now play out the capacity for which it was planned. The activating stage can be created by an assortment of framework occasions, including a check of the quantity of times that this duplicate of the infection has made duplicates of itself.

Execution Phase: This is the real work of the infection, where the "payload" will be discharged. It can be damaging, for example, erasing documents on circle, smashing the framework, or tainting records or generally safe, for example, flying up silly or political messages on screen.

Infection Targets and Replication Techniques: PC infections contaminate an assortment of various subsystems on their host PCs and programming. One way of characterizing infections is to break down whether they dwell in paired executables, (for example, .EXE or .COM records), information records, (for example, Microsoft Word reports or PDF documents), or in the boot part of the host's hard drive.

Resident vs. Non-Resident Viruses: A memory-inhabitant infection (or essentially "occupant infection") introduces itself as a major aspect of the working framework when executed, after which it stays in RAM from the time the PC is booted up to when it is closed down. Inhabitant infections overwrite interfere with taking care of code or different capacities, and when the working framework endeavors to get to the objective record or plate division, the infection code blocks the demand and diverts the control stream to the replication module, contaminating the objective. Conversely, a non-memory-occupant infection (or "non-inhabitant infection"), when executed, examines the circle for targets, taints them, and afterward exits (i.e. it doesn't stay in memory after it is done executing).

Macro Viruses: Numerous normal applications, for example, Microsoft Outlook and Microsoft Word, enable full scale projects to be installed in reports or messages, so that the projects might be run consequently when the archive is opened. A full scale infection (or "archive infection") is an infection that is composed in a large scale dialect, and inserted into these records so that when clients open the document, the infection code is executed, and can taint the client's PC. This is one reason that it is unsafe to open sudden or suspicious connections in messages. While not opening connections in messages from obscure people or associations can lessen the probability of getting an infection, now and again, the infection is composed so that the email seems, by all accounts, to be from a respectable association (e.g., a noteworthy bank or Visa organization).

Boot Sector Viruses: Boot area infections particularly focus on the boot division or potentially the Master Boot Record (MBR) of the host's hard drive or removable stockpiling media (streak drives, floppy plates, and so on.).

Email Virus: An infection that particularly, as opposed to incidentally, utilizes the email framework to spread. While infection contaminated documents might be coincidentally sent as email connections, email infections know about email framework capacities. They for the most part focus on a particular sort of email framework (Microsoft's Outlook is the most regularly utilized), collect email addresses from different sources, and may add duplicates of themselves to all email sent, or may create email messages containing duplicates of themselves as connections.

Stealth Strategies: With a specific end goal to stay away from location by clients, some infections utilize various types of double dealing. Some old infections, particularly on the MS-DOS stage, ensure that the "last changed" date of a host record remains a similar when the document is contaminated by the infection. This approach does not trick antivirus programming, be that as it may, particularly those which keep up and date cyclic repetition minds record changes. Some infections can taint documents without expanding their sizes or harming the records. They achieve this by overwriting unused ranges of executable documents. These are called pit infections. For instance, the CIH infection, or Chernobyl Virus, taints Portable Executable records. Since those records have many purge holes, the infection, which was 1 KB long, did not add to the span of the document.

Read Request Intercepts: While some antivirus programming utilize different methods to counter stealth instruments, once the disease happens any plan of action to "clean" the framework is untrustworthy. In Microsoft Windows working frameworks, the NTFS document framework is exclusive. This leaves antivirus programming minimal option yet to send a "read" demand to Windows OS records that handle such demands. Some infections trap antivirus programming by capturing its solicitations to the Operating framework (OS). An infection can cover up by catching the demand to peruse the contaminated document, taking care of the demand itself, and giving back a uninfected variant of the record to the antivirus programming. The block attempt can happen by code infusion of the genuine working framework documents that would deal with the read ask. In this manner, an antivirus programming endeavoring to recognize the infection will either not be offered consent to peruse the tainted document, or, the "read" demand will be presented with the uninfected form of a similar record. The main solid strategy to stay away from "stealth" infections is to "boot" from a medium that is known to be "perfect".

Security programming can then be utilized to check the lethargic working framework documents. Most security programming depends on infection marks, or they utilize heuristics. Security programming may likewise utilize a database of document "hashes" for Windows OS records, so the security programming can distinguish adjusted records, and demand Windows establishment media to supplant them with real forms. In more seasoned renditions of Windows, document cryptographic hash elements of Windows OS records put away in Windows—to permit record trustworthiness/credibility to be checked—could be overwritten so that the System File Checker would report that changed framework records are valid, so utilizing document hashes to filter for adjusted records would not generally ensure finding a contamination.

Self-Modification: Most current antivirus programs attempt to discover infection designs inside conventional projects by checking them for purported infection marks. Tragically, the term is deceiving, in that infections don't have one of kind marks in the way that individuals do. Such an infection "mark" is just a grouping of bytes that an antivirus program searches for in light of the fact that it is known to be a piece of the infection. A superior term would be "inquiry strings". Diverse antivirus projects will utilize distinctive inquiry strings, and surely extraordinary pursuit techniques, while recognizing infections. On the off chance that an infection scanner finds such an example in a document, it will perform different checks to ensure that it has found the infection and not only a circumstantial arrangement in a blameless record, before it advises the client that the record is tainted. The client can then erase, or (now and again) "clean" or "mend" the tainted record. Some infections utilize methods that make discovery by methods for marks troublesome yet most likely not inconceivable. These infections change their code on every contamination. That is, each tainted record contains an alternate variation of the infection.

Encrypted Viruses: One strategy for dodging mark location is to utilize straightforward encryption to encipher (encode) the body of the infection, leaving just the encryption module and a static cryptographic key in cleartext which does not change starting with one contamination then onto the next. For this situation, the infection comprises of a little unscrambling module and a scrambled duplicate of the infection code. In the event that the infection is scrambled with an alternate key for each contaminated document, the main piece of the infection that remaining parts consistent is the decoding module, which would (for instance) be annexed to the end. For this situation, an infection scanner can't straightforwardly recognize the infection utilizing marks, however it can even now distinguish the decoding module, which still makes circuitous discovery of the infection conceivable. Since these future symmetric keys, put away on the contaminated host, it is totally conceivable to decode the last infection, however this is most likely not required, since self-changing code is such an irregularity, to the point that it might be purpose behind infection scanners to in any event "signal" the record as suspicious. An old yet smaller way will be the utilization of number juggling operation like expansion or subtraction and the utilization of legitimate conditions, for example, XOR operation of digital electronics, where every byte in an infection is with a steady, so that the restrictive or operation had just to be rehashed for unscrambling. It is suspicious for a code to adjust itself, so the code to do the encryption/decoding might be a piece of the mark in numerous infection definitions.

Polymorphic Code: Polymorphic code was the principal system that represented a genuine danger to infection scanners. Much the same as standard encoded infections, a polymorphic infection taints documents with a scrambled duplicate of itself, which is decoded by an unscrambling module. On account of polymorphic infections, be that as it may, this unscrambling module is additionally changed on every contamination. An elegantly composed polymorphic infection hence has no parts which stay indistinguishable between contaminations, making it extremely hard to identify straightforwardly utilizing "marks". Antivirus programming can distinguish it by unscrambling the infections utilizing an emulator, or by factual example examination of the scrambled infection body. To empower polymorphic code, the infection needs to have a polymorphic motor (likewise called "changing motor" or "transformation motor") some place in its encoded body. See polymorphic code for specialized detail on how such motors work. Some infections utilize polymorphic code in a way that compels the transformation rate of the infection essentially. For instance, an infection can be customized to transform just marginally after some time, or it can be modified to avoid changing when it contaminates a document on a PC that as of now contains duplicates of the infection. The benefit of utilizing such moderate polymorphic code is that it makes it more troublesome for antivirus experts and specialists to acquire agent tests of the infection, since "snare" records that are contaminated in one run will commonly contain indistinguishable or comparative examples of the infection. This will make it more probable that the location by the infection scanner will be temperamental, and that a few occurrences of the infection might have the capacity to stay away from identification.

Metamorphic code: To abstain from being identified by imitating, some infections rework themselves totally each time they are to contaminate new executables. Infections that use this procedure are said to be in transformative code. To empower changeability, a "transformative motor" is required. A transformative infection is typically huge and complex.

Vulnerabilities and Infection Vectors:

Software Bugs: As programming is frequently composed with security elements to forestall unapproved utilization of framework assets, numerous infections must endeavor and control security bugs, which are security surrenders in a framework or application programming, to spread them and contaminate different PCs. Programming improvement systems that create extensive quantities of "bugs" will for the most part additionally deliver potential exploitable "openings" or "passages" for the infection.

Social Engineering And Poor Security Practices: With a specific end goal to repeat itself, an infection must be allowed to execute code and keep in touch with memory. Hence, numerous infections connect themselves to executable records that might be a piece of honest to goodness programs. On the off chance that a client endeavors to dispatch a contaminated program, the infection's code might be executed at the same time. In working frameworks that utilization document expansions to decide program affiliations, the augmentations might be avoided the client naturally. This makes it conceivable to make a document that is of an alternate sort than it appears to the client.

Vulnerability of Different Operating Systems: By far most of infections target frameworks running Microsoft Windows. This is because of Microsoft's huge piece of the overall industry of desktop PC clients. The assorted qualities of programming frameworks on a system confine the damaging capability of infections and malware. Open-source working frameworks, for example, Linux enable clients to browse an assortment of desktop situations, bundling apparatuses, and so forth, which implies that pernicious code focusing on any of these frameworks will just influence a subset of all clients. Numerous Windows clients are running a similar arrangement of uses, empowering infections to quickly spread among Microsoft Windows frameworks by focusing on similar adventures on extensive quantities of hosts. While Linux and UNIX when all is said in done have dependably locally kept ordinary clients from rolling out improvements to the working framework condition without authorization, Windows clients are for the most part not kept from rolling out these improvements, implying that infections can undoubtedly pick up control of the whole framework on Windows has.

Counter Measures:

Antivirus Software: By a long shot the greater part of diseases target structures running Microsoft Windows. This is a direct result of Microsoft's tremendous bit of the general business of desktop PC customers. The different characteristics of programming structures on a framework limits the harming capacity of contaminations and malware. Open-source working systems, for instance, Linux empower customers to peruse a variety of desktop circumstances, packaging mechanical assemblies, et cetera., which infers that malicious code concentrating on any of these structures will simply impact a subset of all customers. Various Windows customers are running a comparable game plan of employments, enabling diseases to rapidly spread among Microsoft Windows structures by concentrating on comparative enterprises on broad amounts of hosts.

While Linux and UNIX when all is said in done have reliably privately shielded customary customers from taking off upgrades to the working structure condition without approval, Windows customers are generally not kept from revealing these changes, inferring that contaminations can without a doubt get control of the entire system on Windows has.

Recovery Strategies and Methods: One may lessen the harm done by infections by making consistent reinforcements of information (and the working frameworks) on various media, that are either kept detached to the framework (more often than not, as in a hard drive), read-just or not open for different reasons, for example, utilizing diverse document frameworks. Along these lines, if information is lost through an infection, one can begin again utilizing the reinforcement (which will ideally be later). In the event that a reinforcement session on optical media like CD and DVD is shut, it moves toward becoming perused just and can never again be influenced by an infection (inasmuch as an infection or tainted document was not duplicated onto the CD/DVD).

Virus Removal: Numerous sites keep running by antivirus programming organizations give free online infection checking, with constrained "cleaning" offices (all things considered, the reason for the sites is to offer antivirus items and administrations). A few sites-like Google auxiliary VirusTotal.com—enable clients to transfer at least one suspicious records to be filtered and checked by at least one antivirus programs in one operation. Also, a few able antivirus programming projects are accessible for nothing download from the Internet (normally limited to non-business utilize). Microsoft offers a discretionary free antivirus utility called Microsoft Security Some infections debilitate System Restore and other vital Windows devices, for example, Task Manager and CMD. A case of an infection that does this is CiaDoor.

Operating System Reinstallation: Microsoft's System File Checker (enhanced in Windows 7 and later) can be utilized to check for, and repair, tainted framework documents. Reestablishing a prior "clean" (infection free) duplicate of the whole segment from a cloned plate, a circle picture, or a reinforcement duplicate is one arrangement-reestablishing a prior reinforcement plate "picture" is generally easy to do, as a rule evacuates any malware, and might be quicker than "purifying" the PC - or reinstalling and reconfiguring the working framework and projects starting with no outside help, as depicted underneath, then reestablishing client inclinations. Reinstalling the working framework is another way to deal with infection evacuation.

Viruses and the Internet: Before PC systems wound up noticeably across the board, most infections spread on removable media, especially floppy circles. In the beginning of the PC, numerous clients consistently traded data and projects on floppies. Some infections spread by contaminating projects put away on these circles, while others introduced themselves into the plate boot area, guaranteeing that they would be run when the client booted the PC from the circle, normally accidentally. PCs of the period would endeavor to boot first from a floppy on the off chance that one had been left in the drive. Until floppy plates dropped out of utilization, this was the best contamination technique and boot segment infections were the most widely recognized in the "wild" for a long time. Conventional PC infections risen in the 1980s, driven by the spread of PCs and the resultant increment in release board framework (BBS), modem utilize, and programming sharing. Release board–driven programming sharing contributed straightforwardly to the spread of Trojan stallion projects, and infections were composed to taint prominently exchanged programming. Shareware and contraband programming were similarly basic vectors for infections on BBSs. Infections can expand their odds of spreading to different PCs by tainting records on a system document framework or a document framework that is gotten to by different PCs.

Full scale infections have turned out to be normal since the mid-1990s. The vast majority of these infections are composed in the scripting dialects for Microsoft projects, for example, Microsoft Word and Microsoft Excel and spread all through Microsoft Office by contaminating archives and spreadsheets. Since Word and Excel were likewise accessible for Mac OS, most could likewise spread to Macintosh PCs. albeit the vast majority of these infections did not be able to send tainted email messages, those infections which took preferred standpoint of the Microsoft Outlook Component Object Model (COM) interface. Some old forms of Microsoft Word enable macros to repeat themselves with extra clear lines. On the off chance that two full scale infections at the same time taint an archive, the blend of the two, if additionally self-repeating, can show up as a "mating" of the two and would likely be identified as an infection interesting from the "guardians".

An infection may likewise send a web address interface as a text to every one of the contacts (e.g., companions and associates' email addresses) put away on a tainted machine. In the event that the beneficiary, thinking the connection is from a companion (a confided in source) takes after the connection to the site, the infection facilitated at the site might have the capacity to taint this new PC and keep spreading. Infections that spread utilizing cross-site scripting were first detailed in 2002, and were scholastically shown in 2005. There have been various occasions of the cross-webpage scripting infections in the "wild", misusing sites, for example, MySpace (with the Samy worm).

7.10 Introduction to Cryptography

Cryptography alluded solely to encryption, which is the way toward changing over standard data (called plaintext) into muddled content (called ciphertext). Decoding is the turn around, at the end of the day, moving from the confused ciphertext back to plaintext. A figure (or figure) is a couple of calculations that make the encryption and the switching decoding. The point by point operation of a figure is controlled both by the calculation and in each example by a "key". The key is a mystery (in a perfect world known just to the communicants), normally a short series of characters, which is expected to decode the ciphertext. Formally, a "cryptosystem" is the requested rundown of components of limited conceivable plaintexts, limited conceivable cyphertexts, limited conceivable keys, and the encryption and unscrambling calculations which compare to each key. Keys are essential both formally and in real practice, as figures without variable keys can be inconsequentially broken with just the learning of the figure utilized and are in this way pointless (or considerably counter-beneficial) for generally purposes. Generally, figures were regularly utilized straightforwardly for encryption or unscrambling without extra strategies, for example, validation or respectability checks. There are two sorts of cryptosystems: symmetric and lopsided. In symmetric frameworks a similar key (the mystery key) is utilized to scramble and unscramble a message. Information control in symmetric frameworks is speedier than hilter kilter frameworks as they for the most part utilize shorter key lengths. Uneven frameworks utilize an open key to encode a message and a private key to unscramble it. In conversational utilize, the expression "code" is frequently used to mean any technique for encryption or disguise of significance. Notwithstanding, in cryptography, code has a more particular significance. It implies the substitution of a unit of plaintext (i.e., an important word or expression) with a code word.

7.11 Self Learning Exercise

Q.1 In computer security, ……………………. means that computer system assets can be modified only by authorized parities.

a) Confidentiality

b) Integrity

c) Availability

d) Authenticity

Q.2 In computer security, …………………….. means that the information in a computer system only be accessible for reading by authorized parities.

a) Confidentiality

b) Integrity

c) Availability

d) Authenticity

Q.3 The type of threats on the security of a computer system or network are ……………………..

i) Interruption ii) Interception iii) Modification

iv) Creation v) Fabrication

a) i, ii, iii and iv only

b) ii, iii, iv and v only

c) i, ii, iii and v only

d) All i, ii, iii, iv and v

Q.4 Which of the following is independent malicious program that need not any host program?

a) Trap doors

b) Trojan horse

c) Virus

d) Worm

Q.5 The ……….. is code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.

a) Trap doors

b) Trojan horse

c) Logic Bomb

d) Virus

Q.6 The …………….. is code embedded in some legitimate program that is set to "explode" when certain conditions are met.

a) Trap doors

b) Trojan horse

c) Logic Bomb

d) Virus

Q.7 Which of the following malicious program do not replicate automatically?

a) Trojan Horse

b) Virus

c) Worm

d) Zombie

Q.8 ………….. programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.

a) Zombie

b) Worm

c) Trojan Horses

d) Logic Bomb

Q.9 State whether true of false.

i) A worm mails a copy of itself to other systems.

ii) A worm executes a copy of itself on another system.

a) True, False

b) False, True

c) True, True

d) False, False

Q.10 A ………….. is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs.

a) Worm

b) Virus

c) Zombie

d) Trap doors

7.12 Summary

- ***Viruses:*** Assailants can create destructive code known as infections. Utilizing hacking procedures, they can break into frameworks and plant infections. Infections as a rule are a danger to any condition. They come in various structures and despite the fact that not generally noxious, they generally take up time. Infections can likewise be spread by means of email and circles.
- ***Trojan horses:*** These are vindictive projects or programming code covered up inside what resembles a typical program. At the point when a client runs

the ordinary program, the concealed code keeps running also. It can then begin erasing documents and making other harm the PC. Trojan steeds are regularly spread by email connections. The Melissa infection that brought on dissent of-administration assaults all through the world in 1999 was a sort of Trojan steed.

- ***Worms:*** These are projects that run autonomously and go from PC to PC crosswise over system associations. Worms may have segments of themselves running on a wide range of PCs. Worms don't change different projects, in spite of the fact that they may convey other code that does.
- ***Password cracking:*** This is a procedure assailant's utilization to surreptitiously pick up framework access through another client's record. This is conceivable on the grounds that clients regularly select feeble passwords. The two noteworthy issues with passwords are the point at which they are anything but difficult to figure in view of learning of the client (for instance, spouse's family name) and when they are powerless to lexicon assaults (that is, utilizing a word reference as the wellspring of speculations).
- ***Denial-of-service attacks:*** This assault abuses the need an administration accessible. It is a developing pattern on the Internet since Web locales when all is said in done are open entryways prepared for manhandle. Individuals can without much of a stretch surge the Web server with correspondence so as to keep it occupied. In this way, organizations associated with the Internet ought to plan for (DoS) assaults.
- ***E-mail hacking:*** Electronic mail is a standout amongst the most famous elements of the Internet. With access to Internet email, somebody can conceivably compare with any of a great many individuals around the world.

Some of the threats associated with e-mail are:

- ***Impersonation:*** The sender address on Internet email can't be trusted on the grounds that the sender can make a false return address. Somebody could have adjusted the header in travel, or the sender could have associated straightforwardly to the Simple Mail Transfer Protocol (SMTP) port on the objective PC to enter the email.

- ***Eavesdropping:*** Email headers and substance are transmitted free content if no encryption is utilized. Thus, the substance of a message can be perused or adjusted in travel. The header can be adjusted to stow away or change the sender, or to divert the message.
- ***Packet replay:*** This alludes to the recording and retransmission of message parcels in the system. Bundle replay is a noteworthy danger for projects that require verification groupings, in light of the fact that an interloper could replay real validation succession messages to access a framework. Parcel replay is as often as possible imperceptible, however can be anticipated by utilizing bundle time stamping and parcel arrangement tallying.
- ***Packet modification:*** This includes one framework blocking and adjusting a bundle bound for another framework. Parcel data may not exclusively be adjusted, it could likewise be devastated.
- ***Eavesdropping:*** This permits a saltine (programmer) to make a total duplicate of system movement. Therefore, a saltine can get delicate data, for example, passwords, information, and systems for performing capacities. It is workable for a saltine to spy by wiretapping, utilizing radio, or utilizing helper ports on terminals. It is additionally conceivable to listen stealthily utilizing programming that screens bundles sent over the system. By and large, it is hard to identify listening in.
- ***Social engineering:*** This is a typical type of breaking. It can be utilized by outcasts and by individuals inside an association. Social designing is a programmer term for deceiving individuals into uncovering their secret word or some type of security data.
- ***Intrusion attacks:*** In these assaults, a programmer utilizes different hacking apparatuses to access frameworks. These can extend from secret key splitting devices to convention hacking and control apparatuses. Interruption recognition apparatuses regularly can identify changes and variations that happen inside frameworks and systems.

- ***Network spoofing:*** In system satirizing, a framework presents itself to the system as if it were an alternate framework (PC A mimics PC B by sending B's address rather than its own). The explanation behind doing this is frameworks have a tendency to work inside a gathering of other confided in frameworks. Trust is bestowed in a balanced manner; PC A trusts PC B (this does not infer that framework B trusts framework A). Inferred with this trust is that the framework overseer of the trusted framework is playing out the employment legitimately and keeping up a fitting level of security for the framework. Arrange mocking happens in the accompanying way: if PC A trusts PC B and PC C parodies (imitates) PC B, then PC C can increase generally denied access to PC A.

7.13 Glossary

Spyware : Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive

Bug : An error in a computer program or system.

Encrypt : Convert (information or data) into a code, especially to prevent unauthorized access.

7.14 Answers to Self Learning Exercise

Q.1 (b)

Q.2 (a)

Q.3 (c)

Q.4 (d)

Q.5 (a)

Q.6 (c)

Q.7 (a)

Q.8 (c)

Q.9 (c)

Q.10 (b)

7.15 Exercise

Q.1 What is Virus? Explain its infection methods in Computer.

Q.2 Explain the security methods to protect computer by malware.

Q.3 Explain various types of threats.

Q.4 Explain different protection schemes from worm virus in machines.

Q.5 What are the different security models in email for privacy?

Q.6 Explain the working of antivirus software?

Q.7 Explain about the firewall and Microsoft facilities for security?

References and Suggested Readings

1. Practical UNIX and Internet Security, 3E, Simson Garfinkel (Author), Gene Spafford (Author), Alan Schwartz.
2. Malware: Fighting Malicious Code by Ed Skoudis (Author), Lenny Zeltser .
3. Cryptography and Network Security: Principles and Practice, 6e by William Stallings.
4. Applied Cryptography: Protocols, Algorithms and Source Code in C, 2ed by Bruce Schneier.

UNIT-8

Security Tool in E-Commerce

Structure of the Unit

8.0 Objective

In this chapter we shall focus upon the following topics

- Firewalls & its types
- Configuration of firewalls
- Limitations of Firewall
- Data and Transaction security

8.1 Introduction

- A trend has been observed from the recent studies in the past 8 years: there is a gradual increase in (quality and number of) threats which are related to multi-tier applications/ client-server, that are adopted in Web 2.0 applications.
- Complex scenarios occur because preventions are required for the study of software components and for their communication too.

- Browser and Web server are always critical components.
- Some other possible critical components that may be required are DBMS server and application server.

Web Security:-

- The web presents or constitutes some additional security troubles because:
  - many different computers are involved in any networked domain or framework;
  - the underlying protocols of the Internet were not drafted with security in mind; and,
  - physical infrastructure of the Internet is not owned or maintained by any organization, and no assurance or promises can be made regarding the wholeness, security and reliability of any section of the Internet.
- Unfortunately, a system which is web-based is often proclaimed as to be "secure", the reason being the web server uses SSL encoding techniques to safeguard portions of the site.

Layers Involved in Web Security:

- Many "layers" are involved to produce a functioning web-based system. Each layer has its own security proneness, and its own strategies and approach for managing and coping up with these vulnerabilities.
- Each layer is to be examined, beginning from the hardware which is farthest from the end user to the web browser being closest to the end user.
- If in case one such weakness does not expose these service to attack, that weakness in turn can be used for nefarious and other unfair purposes. The complexity of these layers' interaction makes the job of the security professionals much tougher.

Web Security Usage:

- Web is extensively used by business, government and many other individuals

- but Internet & Web are vulnerable and prone to many attacks
- have various categories of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security methods

8.2 Firewalls & Its Types

Introduction

Firewalls are excellent security mechanisms. Appropriate selections and implementations help in setting up a relatively secure barrier between a system and the external environment.

Firewall Characteristics:

The design goals for a firewall are as follows:

1. The first goal is that all the traffic from inside to outside, and vice versa, must pass through the firewall and this is achieved by physically blocking all access to the local network except via the firewall.
2. Only legalized traffic, as defined by the local security policy, is allowed to pass. Various types of firewalls are used to implement different types of security policies.
3. The firewall being immune to penetration implies the use of a hardened system with a secured operating system. Also, for hosting a firewall, trusted computer systems are suitable and are often a demand and requirement in various government applications.

Types of Firewalls:

A firewall may act as a packet filter as it can operate as a positive filter. This positive filter allows only that packet that fulfills a certain criteria, or it can act like a negative filter which rejects the packet that fulfills any particular criteria. On the basis of dependency on the type of firewall, it can also help in examining one or more protocol headers in each packet, the pattern generated by a sequence of packets, or the payload of each packet. In this part, the focus was on the principal of the various firewalls.

Packet Filtering Firewall:

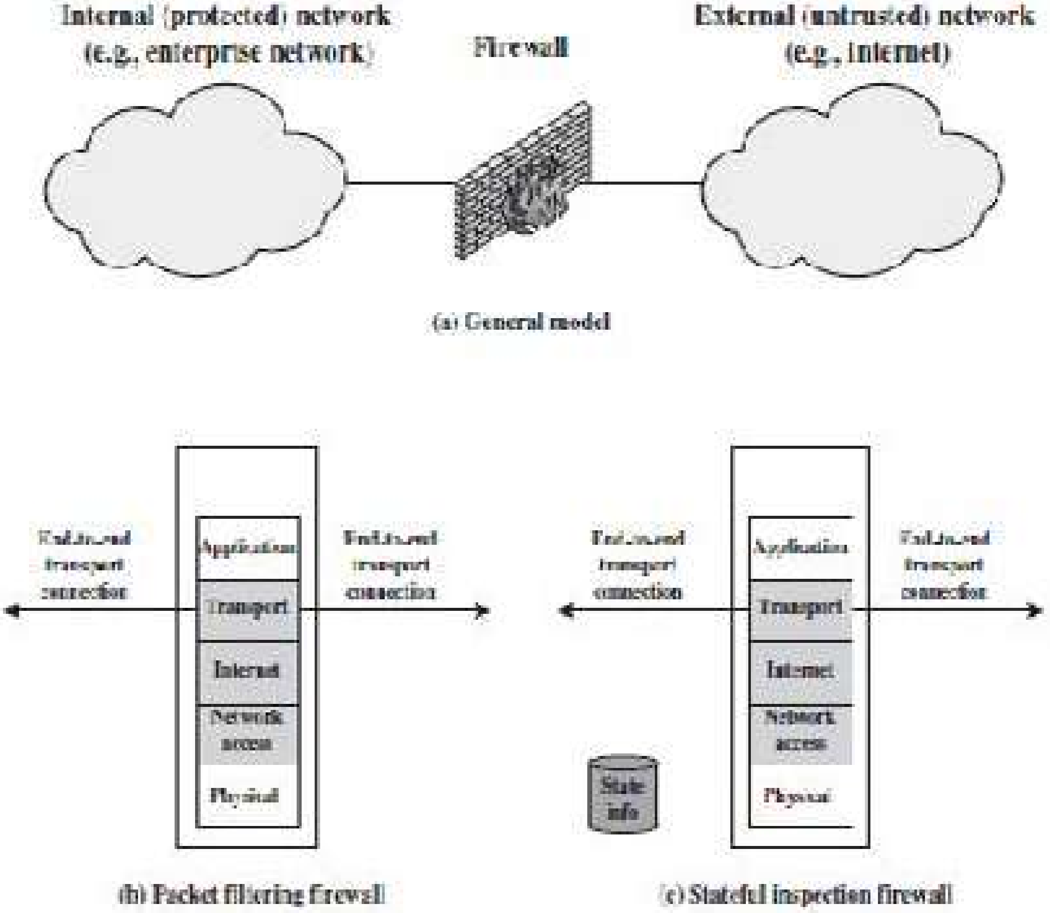
A set of conventional rules is applied to each of the incoming and outgoing IP packet in packet filtering firewall. These packet are also forwarded and discarded by this type of firewall. To filter packets going in both directions (from and to the internal network), the firewall is typically configured for this purpose.

Filtering rules can be described on the basis of the information contained by the network packet:

- **Source IP address**: Source IP address is the IP address of the system from the origin of the IP packet (e.g., 192.178.1.1).
- **Destination IP address:** Destination IP address is the IP address of the system where the IP packet wants to reach (e.g., 192.168.1.2).
- **Transport-level address of Source and destination:** The application such as SNMP or TELNET is defined by the transport-level (e.g., TCP or UDP) port number.
- **IP protocol field:** The transport protocol is defined by this field.
- **Interface:** Here, we consider a firewall with three or more ports, and examine which packet is coming from which of the interface of the firewall or which packet is destined for which interface of the firewall. The packet filter is typically build up as a list of rules or conventions which are based on matches to fields in the IP or TCP header. If there occurs any match to one of the rules, the rule which is invoked is used to determine whether to carry forward or discard the packet. A default action is taken if there is no such match to any rule. Two default approaches are possible which are explained as:
- **Default = discard:** Only that thing is prohibited which is not expressly permitted.
- **Default = forward:** Only that thing is permitted which is not expressly prohibited.

The default discard policy is more conservative in comparison to the default forward policy. Blocking condition is there initially, and after that the services must be added accordinglybased on the cases. This policy is made more visible to the users who are more likely to see firewall as a hindrance. However, this policy is likely to be adopted and implemented by businesses and government organizations. And moreover, as rules are created the visibility to users diminishes. For the end users, the default forward policy increases the ease of use but reduces the security; the security administrator must react to the every new occurring security threat. Various other organizations that is open, like university use this policy.

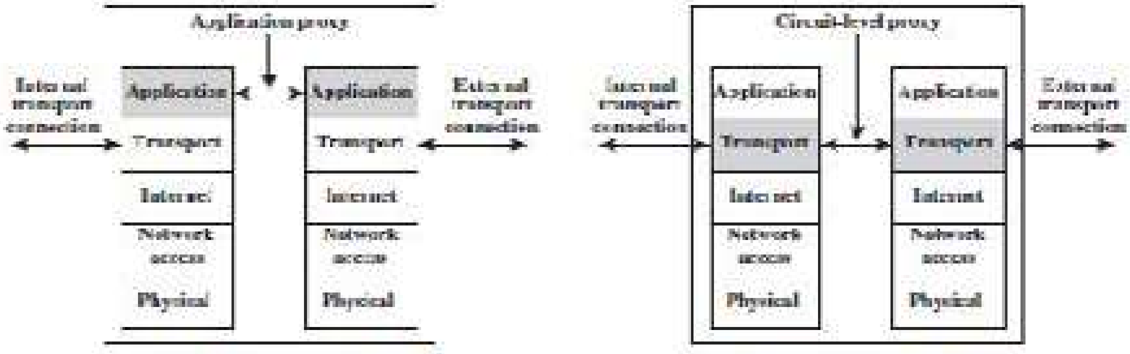
Some of the examples of the packet filtering rule sets are given below.


Internal (protected) network
(e.g., enterprise network)
Firewall
External (untrusted) network
(e.g., Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info
End-to-end transport connection

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall



(d) Application proxy firewall

(e) Circuit-level proxy firewall

Figure 8.1:Types of Firewalls

Rule Set A

Action	Ourhost	port	theirhost	port	comment
Block	*	*	SPIGOT	*	we don't trust these people
Allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

Action	Ourhost	port	theirhost	port	comment
Block	*	*	*	*	default

Rule Set C

Action	Ourhost	port	theirhost	port	comment
Allow	*	*	*	25	connection to their SMTP port

Rule Set D

Action	Src	port	Dest	port	flags	comment
Allow	{our hosts}	*	*	25		our packets to their SMPTP port
Allow	*	25	*	*	ACK	their replies

Rule Set E

Action	Src	port	Dest	port	flags	comment
Allow	{our hosts}	*	*	*		our outgoing calls
Allow	*	*	*	*	ACK	replies to our calls
Allow	*	*	*	>1024		traffic to nonservers

In every set, top to bottom approach is used to apply the rules. A wildcard designator that matches everything is denoted by this field "*".Here, we make an assumption that the default policy is equal to discard policy is in force.

A. Allowance to the inbound mail is made (port 25 is for SMTP incoming) only to a gateway host. The host keeps a history of sending massive files in e-mail messages; for this reason packets from a particular external host, SPIGOT, are blocked.

B. This is basically an explicit statement of the default policy. This rule is included implicitly as the last rule in all the rule sets.

C. This rule set is also purposeful in the sense that it specifies that a mail can be send to the outside by the inside host. A TCP packet carries with itself a destination port of 25 and is routed to the SMTP server which is on the destination machine. The one demerit of this rule is that use of port 25 for SMTP receipt is only a default; however, to have some other application linked to port 25, an outside machine could be configured for this purpose. But one trouble which comes is that an attacker could easily gain access to internal machines by sending packets with a TCP source port number of 25.

D. This rule set offers an advantage that it achieves the intended result that was not achieved in C. A feature of TCP connections is also used by these rules. The ACK flag of a TCP segment is set once a connection is set up, which performs the function of acknowledging segments sent from the other side. Thus, in this rule set, the IP packets are allowed wherein the destination TCP port number is 25 and the source IP address is one of a list of the designated internal hosts. It also provides the allowance of incoming packets which have a source port number of 25 that includes the ACK flag in the TCP segment. Note that to define these rules explicitly, we explicitly designate the source and destination systems.

E. This rule set works on the process to handle FTP connections. Two TCP connections can be used with FTP: first is, a control connection which is used to set up the file transfer and second is, a data connection for providing the actual file transfer; a data connection makes use of a different port number which is assigned dynamically for transfer. However, these low-numbered ports are used by most servers and the attack targets; on the other hand, higher-numbered ports are used by most outgoing calls which should be typically above 1023. Thus, this rule set allows:

- Internally originated packets,
- A connection to which the packets are to be replied which is initiated by an internal machine.
- Packets which are destined for a high-numbered port on an internal machine. This scheme claims a requirement that the systems must be set up so that when needed only the appropriate port numbers are in use.

There is a difficulty pointed out by Rule set E which happens while dealing with applications at the packet filtering level. An alternate way to deal with FTP and similar applications is either an application-level gateway or the stateful packet filters.

One good advantage of a packet filtering firewall is that it's simple to use. Packet filters are efficient in a way that they provide transparency to the users and are actually very fast. [WACK02] lists some weaknesses of packet filter firewalls:

- Packet filter firewalls don't perform the examination of the upper-layer data and are not efficient in preventing those attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot do the blocking of some specific application commands; if a packet filter firewall allows any given application, so that permission to all the functions which are available within that particular application will be allotted.
- The logging functionality which is present in packet filter firewalls is limited, the reason being the limited information being available to the firewall. The access control decisions (source address, destination address,

and traffic type) are made using the same information which is contained in these packet filter logs.

- Most packet filter firewalls don't support the advanced user authentication schemes; the reason being the lack of an upper-layer functionality which is provided by the firewall.
- Packet filter firewalls are prone to attacks and exploits that may take advantage of problems such as *network layer address spoofing* which may occur within the TCP/IP specification and protocol stack. Many are not efficient in detecting a network packet in which the OSI Layer 3 which addresses information has been altered. Spoofing attacks are generally employed by the intruders to bypass the security controls which are implemented in a firewall platform.
- Finally, due to the lesser number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper arrangements or organizations. Also, it is easy to configure a packet filter firewall to provide allowance to traffic types, sources, and destinations that should be denied according to the organization's information security policy.

Some attacks that may occur affecting the packet filtering firewalls are described as follows and the appropriate counter measures to be adopted are as follows:

- **IP address spoofing:** The intruder transmits packets from the outside with a source IP address field to it containing the address of an internal host. The attacker hopes that the use of a spoofed address will allow penetration of systems that use simple source address security, in which packets from the specific trusted internal hosts are accepted. The counter measure here to be considered is that if the packet arrives on an external interface, the approach is to discard packets with an inside source address. In fact, the implementation of the counter measure is done at the router external to the firewall.
- **Source routing attacks:** A packet should follow the route specified by the source station as it crosses the Internet, the possibility being that this will

help to bypass the security measures that don't analyze the source routing information. The counter measure that should be followed here is to discard all the packets that follow this option.

- **Tiny fragment attacks:** The intruder makes use of this IP fragmentation option to create extremely smaller fragments. The TCP header information is forced into a separate packet fragment using this option. Designing of this attack is basically done to circumvent filtering rules that have a dependency on TCP header information. Typically, on the first fragment of a packet, a packet filter will make filtering decision. All the succeeding fragments of that packet are filtered out solely based on this rule that they are part of the packet whose first fragment was rejected. The attacker hopes that the filtering firewall examines and analyses only the first fragment and all the remaining fragments are passed through. A tiny fragment attack can be avoided and controlled by implementing a rule that explains that a predefined minimum amount of the transport header must be contained in the first fragment of a packet. Also, the filter can well remember the packet and discard all subsequent fragments if the first fragment is rejected.

Stateful Inspection Firewalls:

A traditional packet filter makes filtering decisions on an individual packet. It does not take into concern any higher layer context. To understand why a traditional packet filter is limited with regard to context and what is actually meant by *context,* a little background is required. Most standardized applications running on top of TCP follow a client/server approach. For example, for the Simple Mail Transfer Protocol (SMTP), e-mail is transmitted from a client system to a server system. The client system generates new e-mail messages from user input. The server system accepts incoming e-mail messages from the client system. It afterwards places them in the appropriate user mailboxes. SMTP operates by setting up a TCP connection between client and server system, in which there is SMTP server application which is identified by the TCP server port number, the 25 is the TCP port number. The port number of TCP for SMTP client lies between 1024 and 65535 which is produced by the SMTP client. Furthermore, whenever an application uses TCP, it a session is created with a remote host, it also creates a TCP connection which has the TCP port number for the local (client) application is a number that lies in between 1024 and 65535 and the port number for TCP the remote (server) applications have a number less than 1024. Number in between 1024 and 65535 are dynamically generated and have a temporary significance only for the lifetime of a TCP connection and the numbers less than 1024 are the ones which are "well-known" port number and they are permanently assigned to a specific application (e.g., 25 for server SMTP).

Simple packet filtering firewall should allow the inbound network traffic on all the high-numbered port so that TCP-based traffic occurs. It generates a problem of vulnerability which can be exploited by the users that are not authorized.

Thus, a stateful inspection packet firewall is used to tighten up the conventional rule for TCP traffic by generating a directory of the outbound TCP connection, as shown in the Table. For each currently established connection, there is an entry. The packet filter will then allow the incoming traffic to high-numbered port only for that packet that is befitting to the profile of one of the entry in the directory.

Stateful packet inspection firewall does the following job by reviewing the same packet data as a packet filtering firewall, but it also record the information that is in it and the details about various TCP connections .Some stateful firewall also keeps the track of the TCP sequences of the number so as to prevent attack which depends on the sequences of the numbers, such as session hijacking. Some performs the inspection of the limited amount of application data for the well-known protocols like FTP, SIPS and IM commands, so to track and identify the related connection.

Application-Level Gateway

An application-level gateway is also referred to as **application proxy** who acts as a relay of application-level traffic .Using a TCP/IP application, the user contacts the gateway, TCP/IP applications such as Telnet or FTP, and the gateway asks the user for the name of the remote host which has to be accessed. When the user responses and provides a valid user ID and authentication data, the gateway informs the application on the remote host and it relays the TCP segments which contains the application data in between the two endpoints.

However, the service is not supported and cannot be forwarded across the firewall if the gateway does not carry out the proxy code for a particular application.

Further, the gateway can be set up to support only explicit features of an application that the network administrator considered to acceptable but not allowing the other entire feature.

Application-level gateway is efficient in way that they are much secured and safer than the packet filters. Rather than to deal with the various given combination that are allowed and the TCP and IP level being prohibited, it needs to examine only some of the allowable application. Furthermore, it is quite easier to log and audit all the incoming traffic at the application level.

The demerit of application-level gateway is that additional processing overhead is there on every connection. In addition to this, two spliced connection are there in between the end users, with gateway at the splice point, and the gateway should also scrutinize and hence all the traffic should be carried forward in both directions.

Table: Example Stateful Firewall Connection State Table [WACK02]

Source Address	**Source Port**	**Destination Address**	**Destination Port**	**Connection State**
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Circuit-Level Gateway

Circuit-level gateway or **circuit-level proxy** is the fourth type of firewall. It is a stand-alone system or it performs unique function through application-level gateway for many applications. In an application gateway, an end-to-end TCP connection is not permissible by circuit level gateway and it sets up two TCP connection, the connection is stabilized by its own and one between the TCP user which is present in inner host and in between the TCP user which is at outer host level. For the first time when the two connections are established, from the gateway TCP segments relays from one connection to the other without checking-on the contents. It provides security function to check validity of the connections.

Benefit of circuit-level gateway is seen in that condition when the internal users are trusted by the system administrator. To support application-level or proxy service on inbound connections and circuit-level functions for outbound connections gateway can be configured. In this configuration, the gateway can encounter the processing overhead of verifying the coming application data for forbidden functions but it does not encounter that overhead on the data which is outgoing. SOCKS package is the example of a circuit-level gateway implementation

[KOBL92]; version 5th of SOCKS is specified in RFC 1928. SOCKS defined by the RFC in the manner given below:

Protocol that is explained here is design in manner so that it can facilitate a framework for application that are based upon client-server model in TCP as well as in UDP domains in a convenient manner and it uses security service of a network firewall.

A "shim-layer" is present between the application layer and the transport layer, and it does not provide network layer gateway services, like passing away of ICMP messages.

The following components SOCKS consists of:

- The SOCKS server often runs using a UNIX-based firewall. Windows systems also provide facility to implement SOCKS.
- The firewall protects the SOCKS client library which runs on internal hosts.

SOCKS-ified versions of several standard client programs are for example TELNET and FTP. SOCKS protocol can be implemented by doing either the use of alternate dynamically loaded libraries or the Client application that are TCP-based are recompiled or re-linked, providing the allowance so that relevant encapsulation routine can be used in the SOCKS library. When a connection to an object is established by a TCP-based client which can only reach through a firewall (it can be determined after the implementation), then it is important for appropriate SOCKS port on the SOCKS server system that a TCP connection is opened.TCP port 1080 locates the SOCKS service. If the request to the establishment of connection succeeds, then the authentication method is used by which a client enters into negotiation and it also authenticate with selected method and after that a relay request is send to it. The request is evaluated by the SOCKS server and either the appropriate connection is established or it is denied. Furthermore, in a similar manner, the UDP exchanges are handled. A TCP connection is opened to provide authentication so that the end-users can forward and receive UDP segment, as long as the TCP connection is open, the UDP segments are forwarded.

Packets at the network layer or, at most, the transport layer which are examined by the basic traffic filtering, which is limited to configured access list implementations, allows permitting or denying the passage of each packet through the firewall. However, the inspection rules are used in CBAC by which we can create and also use these dynamic temporary access lists. Also, at firewall interfaces, temporary openings in the configured access lists are allowed by the dynamic lists. When the traffic for the mentioned and specified user session exits the internal network through the firewall, then these opening are created. These openings allow returning the traffic for the specified session (that would normally be blocked) and this is done back through the firewall.

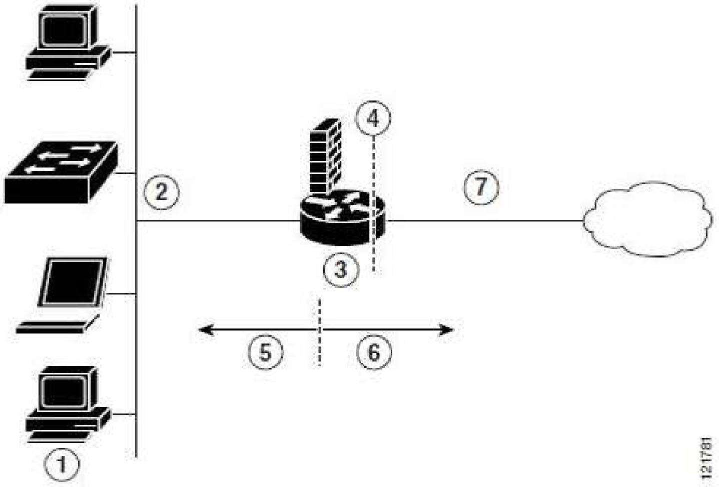


Figure 8.2: Router with Firewall Configured

1. Fast Ethernet LAN interface (the inside interface for NAT)

2. Multiple networked devices—Desktops, laptop PCs, switches
3. PPPoE or PPPoA client and firewall implementation—Cisco 851/871 or Cisco 857/876/877/878series access router, respectively
4. Fast Ethernet or ATM WAN interface (the outside interface for NAT)
5. Unprotected network
6. Protected network
7. Point at which NAT occurs

In the following configuration example, the firewall can be applied to the outside

WAN interface (FE4) on the Cisco 871 or Cisco 851 and it also protects the Fast Ethernet LAN on FE0 by inspecting the traffic which is entering through the router on the Fast Ethernet WAN interface FE4. It is important to note here in this example that, the network traffic originating from the corporate network, network address 10.1.1.0, is considered to be a safe traffic and is not filtered.

Configuration Tasks

To configure this network scenario, the following tasks are performed which are:

- Configure Access Lists
- Configure Inspection Rules
- Apply Access Lists and Inspection Rules to Interfaces

8.4 Limitations of Firewall

It should be kept in mind that the firewall should not be installed and rest you should assure that your information is safe. There are various demerits of firewalls. We already discussed the types of firewalls in the fourth article, explaining that the firewall work is based on the various layers of TCP/IP model of Internet and OSI model of corporate networks to secure the network and/or your computer. In the article on the types of firewalls, it is explained that there should be some convention rules that provides further protection to your computers and networks. Knowledge of ports should be required to create different convention rules. Custom rules are easily created by some firewalls such as the Comodo Internet Firewall (software firewall).

For networks, this thing should be kept in mind that the computers should be exposed to the outside world - other networks or the Internet - via a strong and single firewall.

One computer should be considered as main and a strong protection should be used on it. Any computer within the network should not be allowed to be connected to the external world on its own; rather it should be first connected to the main computer. The main computer act as a server in the client-server model. An operating system should be used for smaller networks that prevent users of other computers from creating parallel connections to Internet (e.g. dial-up connections). Are you completely secured by the above practices? However, the answer to this question is a big NO. After applying so many techniques, there are always some demerits left of firewalls and people still make good use of them. However, your firewall(s) can be configured to reduce risk by applying the approach of "limiting" the "limitations of Firewalls."

Most Common Limitations of Firewall

Architecture is the first and foremost thing in the limitations of firewalls. We know that the various types of firewalls work at various levels of TCP/IP protocol or sometimes at OSI model of networks. Most of the firewalls work only at the topmost layers of these or Network models or Internet, thus it provides security feature at lower level. For example, a firewall which is operating at Application Level of TCP/IP protocol examine the pattern of the data and application signature will let you know whether the packet is safe or not. (If it searches out that application present in the reputed programs list of your operating system, firewall, or previously allowed application list, then the data packet into the computer or network are let in by the firewall). The data packet patterns are easy to exploit if data patterns are observed by the hacker. The hacker can easily create fake packets that contain "trusted source IP" to hack network as well as computer. Such limitations of firewalls can be overcome by creating additional set of convention rules that impels the firewall and helps to scan the data packets in more depth, maybe at a different layers of network. However, we need some knowledge about the network models to create such conventional rules. The most important limitation of firewalls is the configuration of a network. If the configuration of the network is not done in proper manner, the firewall will not be able to perform. If there occurs a fault in network design, then no matter how much you spend on the network safety, the network will fail. This problem can be overcome by the involvement of experienced network designers and we can also restrict the access to other computers by installing a parallel Internet connection like a dial up connection. Anything can be installed via the main computer to overcome this demerit of firewall.

Firewall is a good approach to protect the organization from hackers. But there exist some limitations. The following ten firewall limitations consist of:

- ***Viruses:*** Computer viruses cannot be fully protected by all firewalls as many ways are there to encode files and they can be transferred over the Internet.
- ***Attacks:*** Firewalls don't offer protection against attacks that don't go through the firewall like, the firewall in our system may restrict access from the Internet, but it may not provide protection to your equipment from dial in access to your computer systems.
- ***Architecture:*** Consistent overall organization security architecture: The overall level of security in the network is reflected by the firewall. A single point of failure is there in an architecture that depends upon one method of security or one security mechanism. A failure through a software application bug or in its entirety may make the company vulnerable to intruders.
- ***Configuration:*** A firewall can't give any information that it has been incorrectly configured. Trained professionals have the caliber, experience and talent to properly configure them.
- ***Monitoring:*** If a perceived threat occurs, then firewall notifies us. However, they can't tell you if your network is hacked by someone. There is a need of additional hardware, software and network monitoring tools by many organizations.
- ***Encryption:*** While Virtual Private Networks (VPNs) and firewall are helpful, they don't encrypt E-mail messages and confidential documents sent within the organization or to outside business contacts. However, to

provide protection to the confidential documents and electronic communications, formalized procedures and tools are needed.

- ***Management:*** Incoming threats are restricted by firewalls but organizations still need a formalized archival, destruction and management procedure for their electronic documents. Electronic messages which are out of context can cause financial problem to an organization.
- ***Masquerading:*** A hacker can be masquerade and can act as an employee which is unstoppable by the firewall. Related passwords and user ids can be acquired by the hacker in number of ways.
- ***Policies:*** A strong Security Policy and Procedure Manual cannot be achieved by the firewall. Security structure of an organization depends on how strong the weakest link. The reputation of an organization can be protected by the security professionals as they have a lot of experience.
- ***Vulnerabilities:*** Like a deadbolt lock on a front door, a firewall will not inform you if there occurs vulnerabilities and by that internal network can be accessed by the hacker. Risks can be managed by Security Vulnerability Assessments on which the organization can rely.

8.5 Data and Transaction Security

Security plays an important role in any transaction that takes place over the internet. Customer cannot rely on e-business if its security is compromised anywhere. The essential requirements for safe transactions and e-payments are as follows –

- **Confidential** – Unauthorized person should not be able to access the valuable information. Interception should not be occurring during the transmission.
- **Integrity** – during transmission over the network, information should not be altered.
- **Availability** – Information should be available according to the requirement within the time limit specified.
- **Authenticity** – A user should be identified authentic before giving him/her the access to the required information.

Non-Repudiate – This is the protection against denial of payment or denial of order. The sender should not be able to deny sending the message once a message is send and in the same manner recipient of message should not be able to deny that message is received by them.

Encryption – Authorized user can only encrypt and decrypt the information.

Auditability – for full filling the integrity requirements data is audited so that it can be recorded accordingly.

Measures to Ensure Security:-

Following security measures are taken which are as follows –

- ***Encryption*** – It is a very effective technique to safeguard the data that is being transmitted over the network. Using a secret code, sender of the information encrypts the data and the intended receiver uses the same or different secret code to decrypt the data.
- ***Digital Signature*** – Authenticity of information is ensured by digital signature. A digital signature is an e-signature which is authenticated by using encryption and password.
- ***Security Certificates*** – It is a unique digital id which is used for verification of the identity of a user or an individual website.

Security Protocols in Internet:-

Some popular protocols used over the internet to ensure the security of transactions which are as follows.

Secure Socket Layer (SSL)

It is the most commonly used protocol among the others and it is widely used and implemented in the industrial areas. It meets following security requirements which are named as –

- Authentication
- Encryption
- Integrity
- Non-reputability

"https://" is used for HTTP urls with SSL and "http:/" is used for HTTP urls without SSL.

Secure Hypertext Transfer Protocol (SHTTP)

It is the extension of HTTP internet protocol providing authentication, public key encryption, and digital signature over the internet. It supports multiple security mechanism that provide security to end users. It works by negotiating the types of encryption scheme used between the client and the server.

Secure Electronic Transaction

This is a secure protocol which was developed by Visa and MasterCard in collaboration. Theoretically, this is one of the best security protocol. It consists of the following components−

- **Card Holder's Digital Wallet Software** − Digital Wallet allows secure purchases that can be made using online point and click interface by the card holder.
- **Merchant Software** −This software is used to help merchants which can interact with financial institutions and potential customers in a very secure manner.
- **Payment Gateway Server Software** − Payment gateway helps to standard and automatic payment process. The process of merchant's certificate request is supported by it.
- **Certificate Authority Software** − Financial institutions uses this software to issue digital certificates to merchants and card holders and they can enable account agreements by registering for secure electronic commerce.

8.6 Self Learning Exercise

Q.1 The mechanism to protect private networks from the outside attacks is

a) Firewall

b) Antivirus

c) Digital signature

d) Formatting

Q.2 A proxy firewall filters at the

a) Physical layer

b) Application layer

c) Data link layer

d) Network layer

Q.3 A packet filter firewall filters at the

a) Application or transport layer

b) Data link layer

c) Physical layer

d) Network or transport layer

Q.4 A firewall is a

a) Wall which is built to prevent fires from damaging a corporate intranet

b) Security device which is deployed at the boundary of a company so as to prevent unauthorized physical access

c) Security device which is deployed at the boundary of a corporate intranet in order to protect it from the unauthorized access

d) Device to prevent all accesses from the internet to the corporate intranet

Q.5 A firewall may be implemented in

a) Routers which connect intranet to internet

b) Bridges used in an intranet

c) Expensive modem

d) User's application programs

Q.6 Firewall as part of a router program

a) Filters only packets coming from internet

b) Filters only packets going to internet

c) Filters packets travelling from and to the intranet from the internet

d) Ensures rapid traffic of packets for speedy e-Commerce

8.7 Summary

The successful use of a firewall is totally depends on the appropriate product selection.Packet-filtering firewalls can accept or reject packets which is based on various conventional rules that depends on the destination and source ports of packets and other than this many more criteria do exists. For plug-and-play firewall solution this type of firewall is the closest option and at the same time it is easiest to defeat. Proxy-based firewalls like circuit-gateway firewalls, cannot be defeat able easily, and the last obtained virtual circuit connection is relatively transparent to users. However, the semantics of applications cannot be understood by the circuit gateway firewall and thus some amount of granularity of control is lacking behind. Application gateway firewalls are proxy-based firewall, but a specific application can be connected to a specific client. Granularity of control is provided by Application gateway firewall, but every application that proxies need to be modified, and there is less transparency to users in comparison to circuit gateway firewalls.

8.8 Glossary

Firewall : A firewall creates a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.

Transaction: This is the process that takes place when a cardholder makes a purchase with a credit card.

8.9 Answers to Self Learning Exercise

Q.1 (a)

Q.2 (b)

Q.3 (d)

Q.4 (c)

Q.5 (a)

Q.6 (c)

8.10 Exercise

Q.1 Give the four techniques that firewall uses to enforce security policy and control access?

Q.2 Which type of information a typical packet filtering firewall uses?

Q.3 Mention some of the weaknesses of packet filtering firewalls?

Q.4 State the difference between a packet filtering firewall and a stateful inspection firewall.

References and Suggested Readings

1. Vijay Ahuja, "Building Trust in Electronic Commerce", IEEE/2000, pp: 61-63

2. Stuart Feldman, "The Changing Face of E-Commerce: Extending the Boundaries of the Possible", IEEE INTERNET COMPUTING, MAY JUNE 2000, pp: 82-83

3. Audin, G. "Next-Gen Firewalls: What to Expect." *Business Communications*

   Review, June 2004.

4. Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications*

   Magazine, September 1994.

UNIT-9
Risk Management Approach in E-Commerce

Structure of the Unit

9.0 Objective

In this unit we shall learn the following topics

- Risk in E-Commerce
- Data and Gateways Security

- Handling Transactions
- Policies for website utilities

9.1 Introduction

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

Risk management is relevant to all organizations (public and private, large or small). It should be a part of the culture of the organization, with a program and an effective policy led by top management with transparent responsibilities laid down for every manager and employee to be involved in the management of risk. Risk management supports performance measurement, accountability and reward thus improving efficiency at all levels.

9.2 History

The advent of the e-commerce a decade ago presented retailers with a brand new avenue for selling their goods and services. Existing customers now had an alternative to actually going to a physical store, while online stores now had the world as their market. The other side of the coin is that criminals see the e-commerce as an additional source for gathering sensitive personal information that can be later used for processing fraudulent transactions. Personal data can be compromised or stolen in a number of different ways, but web-based merchants can and should develop risk management procedures and implement them into their sales process to help protect consumer information from falling into the wrong hands. As a step in this direction, and in order to reduce losses resulting from excessive risk exposure, e-commerce merchants must implement internal fraud prevention measures and controls that are designed to their environment's specifics. A dedicated fraud control department can provide the direction that your organization needs, in order to fight fraud effectively.

9.3 Overview

One way to avoid e-commerce problems is to adopt a proactive risk management program. Risk management needs to be recognized as integral activity for e-commerce. Customers are going to have to figure out whether the product is going to sell, what the opportunities are for it, monitor the sales, and so on and then E-Commerce Series: Risk Management for the Internet to monitoring the results. List of risk management areas for e-commerce setup:

1. Asset risk relating to returns
2. Asset liquidity risks
3. Inadequate pricing
4. Regulatory risks
5. Reputation risks
6. Operational risks
7. Strategic risks

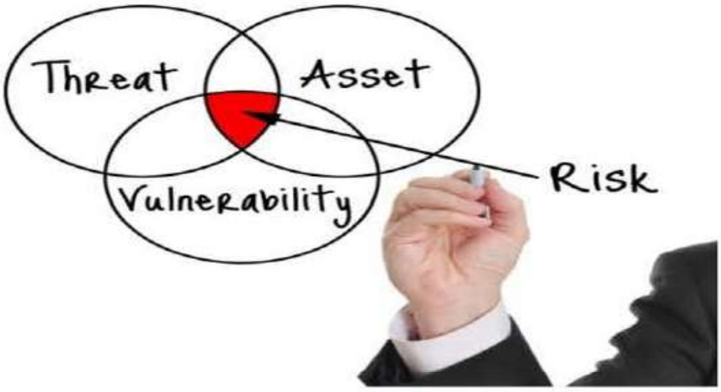


Figure 9.1: Risk management aspects

9.4 Orientation

The management of risk in e-commerce transactions is considered the most important factor for the long term survival of the business. These risks may relate to Internet fraud, information security, payment methods or even e-commerce legislation. Once getting into one of those risks, it would be costly for business to solve and to recover. Business owners should develop an internal policy to address the potential risks and train their staff on implementing it. Following are the most important procedures for managing risk in e-commerce transactions.

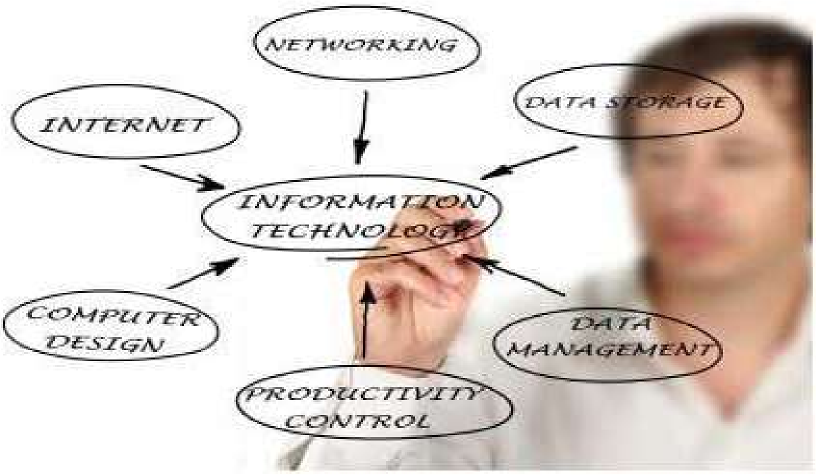


Figure 9.2: Risk management targeted features

9.5 Risks in E-Commerce

Fourteen Steps to Managing E-Commerce Risk Following are the most important procedures for managing risk in E-Commerce transactions:

1. Exposure to E-Commerce risk depends on business policies, operational practices, fraud detection and prevention tools, security controls, and the types of products and services that provided to the customers. Everyone in the organization should understand the risks associated with online transactions and be able to implement their established risk management procedures.
2. **Select the right acquiring bank and merchant services provider.** The right acquiring bank and merchant services provider will provide effective risk management support have a complete understanding of E-Commerce fraud risk and liability. An adequate customer data protection capability is also something considered when making your selection.
3. **Develop essential website content.** Customer website must include privacy, shipping, return and refund policies. It must be reliable and to provide with easy and simple navigation.

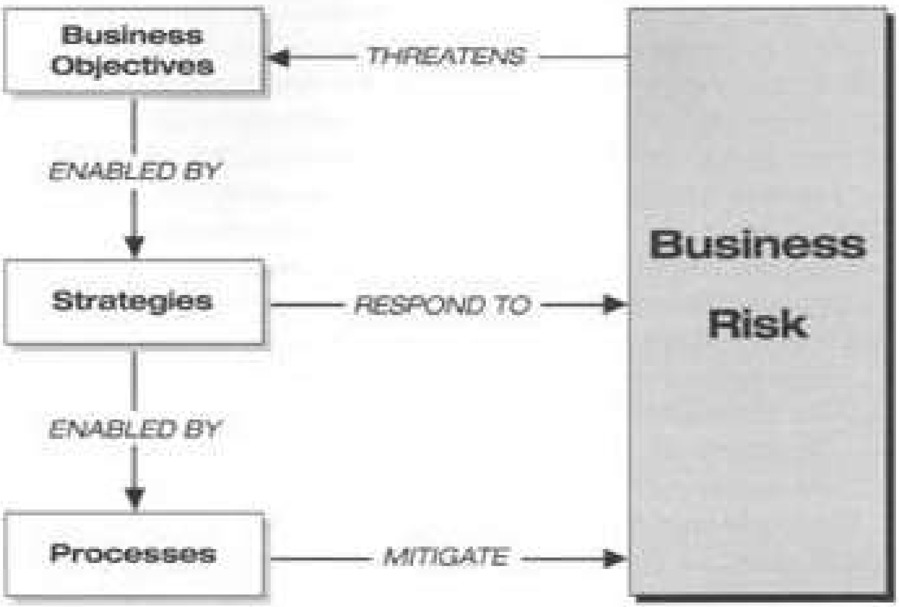


Figure 9.3: Risk management flow chart

4. **Always concentrate on risk reduction.** A properly established sales order process will help to address a number of risk concerns. Properly indicate or highlight required transaction fields and verify card and cardholders data that received from customers over the Internet.

5. **Design and implement internal fraud prevention structure.** The profitability of e-commerce store depends on their internal strategies and controls for minimizing fraud. A risk management structure, combined with intelligent transaction controls, will help to avoid fraud-related losses.

6. **Use fraud-prevention tools.** There are a number of fraud-prevention tools must be used to reduce risk exposure. The most widely used among them are the Address Verification Service (AVS), the Card Security Codes, Verified by Visa an MasterCard, Secure Code.

7. **Apply fraud screening application.** When it is properly implemented, the screening of online card transactions can help to minimize fraud for large-ticket items and for high-risk transactions.

8. **Always protect the merchant account from intrusion.** Implementing proactive measures that can minimize the risk of criminals gaining access to shopping cart details or payment gateway and making fraudulent fund deposits.

9. **Create a secure process for routing authorizations which** need to set up a secure and efficient process for submitting authorization requests over the Internet, before company can start accepting card payments online.

10. **Set up a process for handling transaction post-authorizations which** need an effective process in place for dealing with approved and declined authorizations before fulfilling an order.

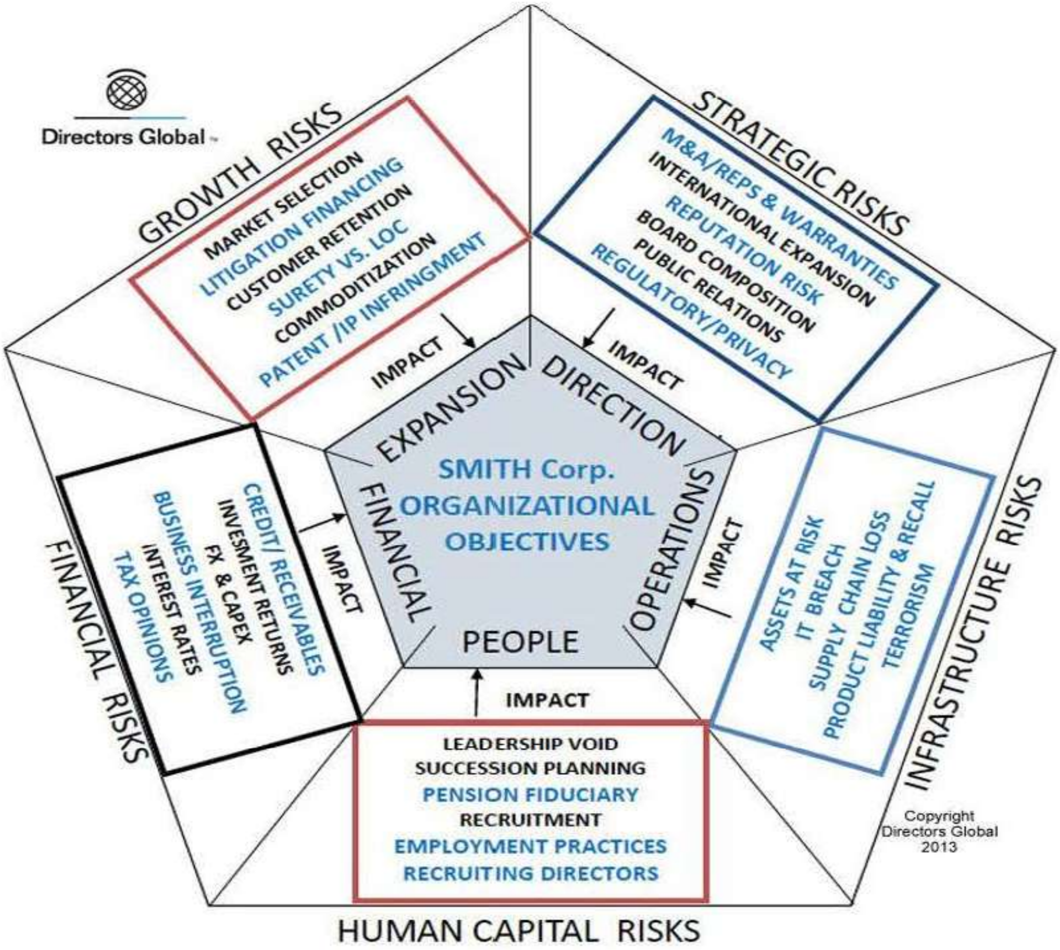


Figure 9.4 : Auditable features for Risk Management of business

11. **Protect card holder information through PCI compliance where** the Payment Card Industry Data Security Standards provide E-Commerce merchants with standards, procedures and tools for data protection. This content need reliable encryption capabilities for data transmission and effective internal controls for protecting stored card and card holder information.

12. **Avoid unnecessary charge backs.** Charge backs represent extra processing time and costs, hurt profits and may result in a loss of revenue. By carefully tracking and managing charge backs.

13. **Monitor charge backs, this means that** Effective chargeback monitoring mechanisms will help to detect excessive chargeback activity, identify the causes, and apply corrective measures to bring chargeback levels down.

14. **Use collection efforts to minimize losses which are a** well-designed collection system that can help to recover unwarranted chargeback losses.

9.6 Data and Gateway Security

Data Security Policy:

Consumers expect that e-commerce merchants protect the personal information which is provided during a transaction. They also expect that merchants describe the measures and procedures that they have established to keep sensitive account data save for a better customer experience. E-Commerce merchants should consider implementing the following best practices on information security:

- **Educate Customers about their Security Practices during transactions.**
- Payment information is protected at all stages of the transaction process during transmission, while on company's server and at their physical work site.
- **Add the Logos of Fraud Prevention Services that are using at p**lace on the website.
- **Warn Customers against Sending Payment Information by Email.**
- To protect their personal information highlight the security practices on the website and in email correspondence.

Payment Gateways Security:

A payment gateway is an e-commerce service that processes credit card payments for online. Payment gateways facilitate these transactions by transferring key information between payment portals such as web-enabled mobile devices/websites and the front end processor/bank and fulfill a vital role in the e-commerce transaction process, authorizing the payment between merchant and customer. A **payment processor** analyzes and transmits transaction data. **Payment gateways** authorize the transfer of funds between buyers and sellers. When a customer places an order from an online store, the payment gateway performs several tasks to finalize the transaction:

- **Encryption:** The web browser encrypts the data to be sent between it and the vendor's web server. The gateway then sends the transaction data to the payment processor utilized by the vendor's acquiring bank.
- **Authorization Request:** The payment processor sends the transaction data to a card association. The credit card's issuing bank views the authorization request can be "approves" or "denies."
- **Filling the Order:** The processor then forwards an authorization pertaining to the merchant and consumer to the payment gateway. Once the gateway obtains this response, it transmits it to the website/interface to process the payment. Here, it is interpreted and an appropriate response is generated. This seemingly complicated and lengthy process typically takes only a few seconds at most. At this point, the merchant fills the order.
- **Clearing Transactions:** The steps outlined above are repeated in an effort to "clear" the authorization via a consummation of the transaction. However, the clearing is only triggered once the merchant has actually completed the transaction (shipping the order). The issuing bank changes to a debit, allowing a "settlement" with the vendor's acquiring bank. The processor is then relied upon to settle all of the vendor's approved authorizations with the acquiring bank at the end of the day.

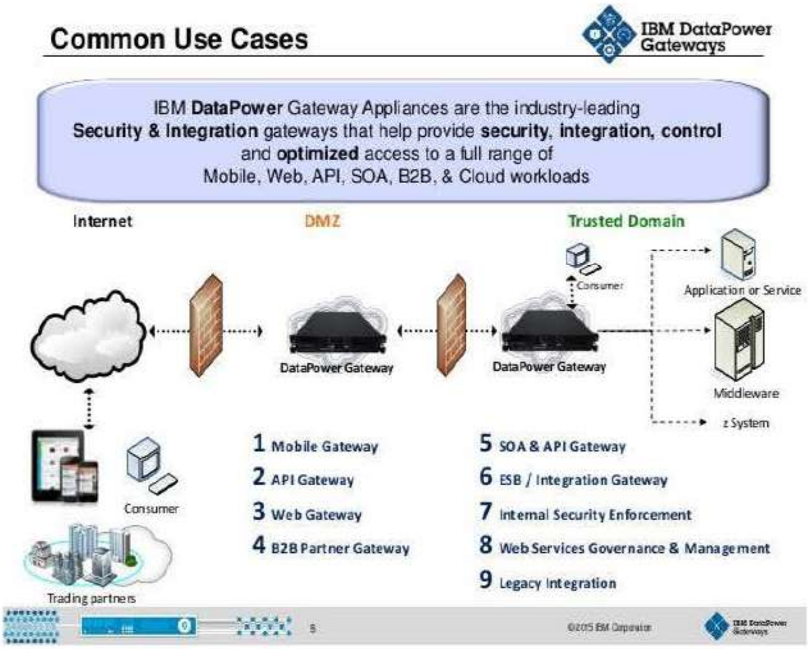
Other Payment Gateway Functions: Payment gateways also screen orders with a myriad of helpful tools. This screening process filters out as much fraud as possible. Examples of gateway fraud detection tools include:

Delivery address verification

- AVS checks
- Computer finger printing technology,
- Velocity pattern analysis
- Identity morphing detection

- Geo location

Payment gateways even calculate tax amounts to authorize requests transmitted to the processor.



Common Use Cases

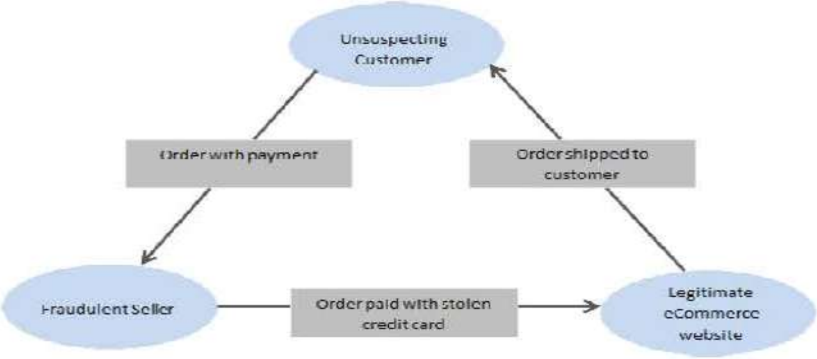
IBM **DataPower** Gateway Appliances are the industry-leading **Security & Integration** gateways that help provide **security, integration, control** and **optimized** access to a full range of Mobile, Web, API, SOA, B2B, & Cloud workloads

1 Mobile Gateway
2 API Gateway
3 Web Gateway
4 B2B Partner Gateway
5 SOA & API Gateway
6 ESB / Integration Gateway
7 Internal Security Enforcement
8 Web Services Governance & Management
9 Legacy Integration

Figure 9.5: Data and Payment Gateway security shown by IBM through IOT

9.7 Fraud Schemes in E-Commerce

There are certain e-commerce transaction characteristics that are statistically very likely to be present when fraud is being committed. If only one or two of these signs are present, this may not be a cause for concern, but if several are identified in a single transaction, the merchant should investigate and verify the validity of both the card and the card holder before processing the payment.



Unsuspecting Customer
Order with payment
Order shipped to customer
Fraudulent Seller
Order paid with stolen credit card
Legitimate eCommerce website

Figure 9.6: Targeted fraud related sectors

1. **First-time shoppers:** Criminals are always looking for new victims. Once they commit a fraud at one merchant, they usually move on to another and never come back.
2. **Larger-than-average orders:** Stolen payment cards have a very limited life span so criminals need to make a quick use of them. Large-size orders are one way of doing that.
3. **Orders for several items of the same kind:** Just as with larger-than-average orders, purchasing multiple items of the same kind is a way of maxing out stolen cards as quickly as possible.
4. **Big-ticket items:** Big-ticket items have high resale value, maximizing the fraudsters' profits.
5. **Orders with overnight delivery:** Naturally, criminals do not much care about shipping costs and are more likely than legitimate shoppers to order items with an overnight or another type of a rushed delivery.
6. **Orders from Internet addresses at free email services:** Free email services have no billing relationship with their users, leaving no possibility for verification that a legitimate card-holder has opened the account.
7. **International shipping addresses:** A substantial number of fraudulent transactions are shipped to international addresses.
8. **Similar account numbers:** There are various software tools for generating card account numbers, such as Credit Master. These numbers are often very similar.
9. **Multiple orders shipped to the same address:** Such orders may indicate the use of a stolen batch of cards or of fraudulently generated account numbers.
10. **Multiple transactions on one card in a short amount of time:** Such transactions may indicate that a criminal is attempting to run up a stolen card's credit line as quickly as possible, before the account is closed.
11. **Multiple shipping addresses:** Similarly to the previous scheme, a card may be used multiple times in a short amount of time with the orders going to several shipping addresses.

12. **Multiple cards from a single IP address:** Such transactions may indicate multiple orders placed from the same computer, even if different names and shipping addresses have been used.

9.8 Handling Transactions

All card-not-present transactions must be authorized before they are processed. The authorization response will typically be an approval or decline. E-commerce merchants need to develop a process for handling transactions after the authorization response is received and apply it consistently.

Obtaining authorization for card-not-present transactions:

Obtaining an authorization is part of the process of verifying the cardholder's identity and the validity of the transaction.

Figure 9.7 : Online Payment mode system

When customer submits their authorization request, consider the following:

- Avoid using an economic authorization to verify if the account is in good standing.
- If the transaction has failed Verified by Visa or MasterCard, Secure Code authentication, do not submit it for authorization, but instead request an alternative payment method.
- Include the card's expiration date in customer's authorization request, but do not submit requests if the card is expired or no expiration date is provided.
- Obtain the card's security code and submit it with the authorization request. Card security codes are the three-digit numbers that are found in the

signature panels on the back of Visa (CVV2), MasterCard (CVC 2) and Discover (CID) cards and the four-digit numbers that are found slightly above and to the right of the account numbers of American Express (CID) cards.

- Obtain the cardholder's billing address. Customer can submit an address verification (AVS) request to the card issuer separately or as part of the authorization request. Customer will receive an AVS response code, separate from the authorization response code.

- **For approved transactions, email their customer an order confirmation:** To reduce customer disputes, include in the order confirmation details about the purchase. This will also enable them to verify the cardholder's email address. If the email address turns out to be invalid, customer should research the situation and determine whether or not the order is legitimate.

- **For declined transactions, review the situation and take appropriate actions:** Consider contacting their customer to obtain corrected information or an alternative payment that may allow customer to complete the sale. Review authorization declines and contact customers to correct problems with their cards or ask them for an alternative payment method. If the card information is corrected, make sure to obtain authorization approval from the card issuer before completing the sale. Regularly evaluate the success of their authorization decline review strategy and modify it, as needed.

- **Monitor customer's transaction decline rates:** This will help customer to identify potential problems in their post-authorization process. If the issues are adequately addressed, their approval rates and sales volumes will both increase, improving customer satisfaction in the process. In particular, customer should: Track their order declines by reason on a daily basis. Separate transactions declined by the card issuer from those declined by you for suspected fraud or other reasons.

- **For approved transactions, email your customer an order confirmation:** To reduce customer disputes, include in the order confirmation details about the purchase. This will also enable you to verify the cardholder's email address. If the email address turns out to be invalid, you should research the situation and determine whether or not the order is legitimate.

9.9 Online Transactions Processing

Credit cards/ Debit cards: It constitutes a popular method of online payment but can be expensive for the merchant to accept because of transaction fees primarily. Debit cards constitute an excellent alternative with similar security but usually much cheaper charges.

Net banking: It is used by customers who have accounts enabled with Internet banking. Instead of entering card details on the purchaser's site, in this system the payment gateway allows one to specify which bank they wish to pay from. Then the user is redirected to the bank's website, where one can authenticate oneself and then approve the payment. Typically there will also be some form of two-factor authentication.

PayPal: PayPal is a global e-commerce business allowing payments and money transfers to be made through the Internet. Online money transfers serve as electronic alternatives to paying with traditional paper methods, such as cheques and money orders.

Figure 9.8: Paypal Card for online payment mode system

Paymentwall: Payment-wall, an e-commerce offers a wide range of online payment methods that its clients can integrate on their website.

Google Wallet: Google Wallet was serving a similar function as PayPal to facilitate payments and transfer money online. It also features a security that has not been cracked to date and the ability to send payments as attachments via email.

Figure 9.9: Mobile/net banking for online payment mode system

Mobile Money Wallets: There are more mobile phone users than there are people with active bank accounts. Telecommunication operators, in such geographies, have started offering mobile money wallets which allows adding funds easily through their existing mobile subscription number, by visiting physical recharge points close to their homes and offices and converting their cash into mobile wallet currency.

9.10 Chargeback in Visa Transaction

A "chargeback" provides an issuer with a way to return a disputed transaction. When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the acquirer, if needed.

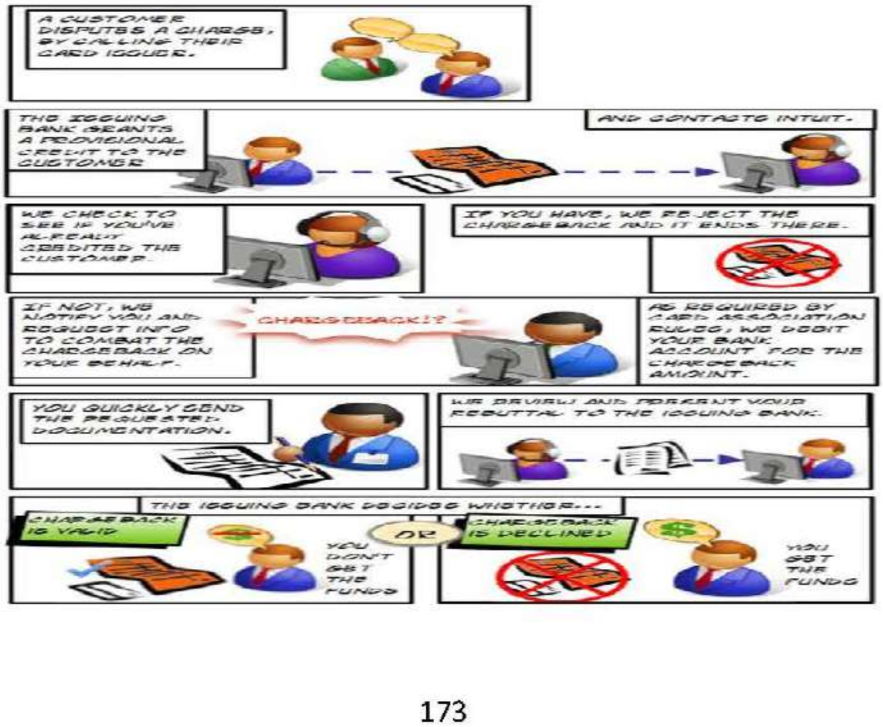

A CUSTOMER DISPUTES A CHARGE, BY CALLING THEIR CARD ISSUER.
THE ISSUING BANK GRANTS A PROVISIONAL CREDIT TO THE CUSTOMER
AND CONTACTS INTUIT.
WE CHECK TO SEE IF YOU'VE ALREADY CREDITED THE CUSTOMER.
IF YOU HAVE, WE REJECT THE CHARGEBACK AND IT ENDS THERE.
IF NOT, WE NOTIFY YOU AND REQUEST INFO TO COMBAT THE CHARGEBACK ON YOUR BEHALF.
CHARGEBACK!?
AS REQUIRED BY CARD ASSOCIATION RULES, WE DEBIT YOUR BANK ACCOUNT FOR THE CHARGEBACK AMOUNT.
YOU QUICKLY SEND THE REQUESTED DOCUMENTATION.
WE REVIEW AND PRESENT YOUR REBUTTAL TO THE ISSUING BANK.
THE ISSUING BANK DECIDES WHETHER...
CHARGEBACK IS VALID
YOU DON'T GET THE FUNDS
OR
CHARGEBACK IS DECLINED
$
YOU GET THE FUNDS

Figure 9.10: Chargeback functioning system

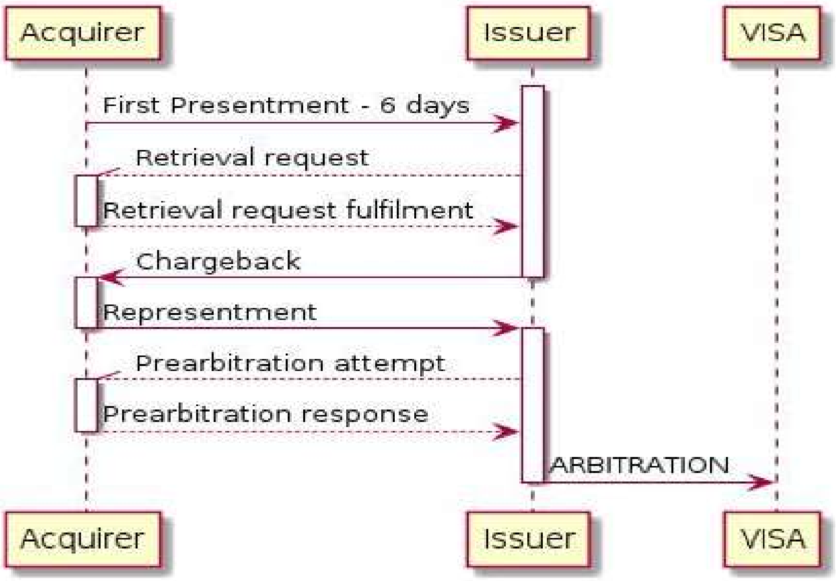
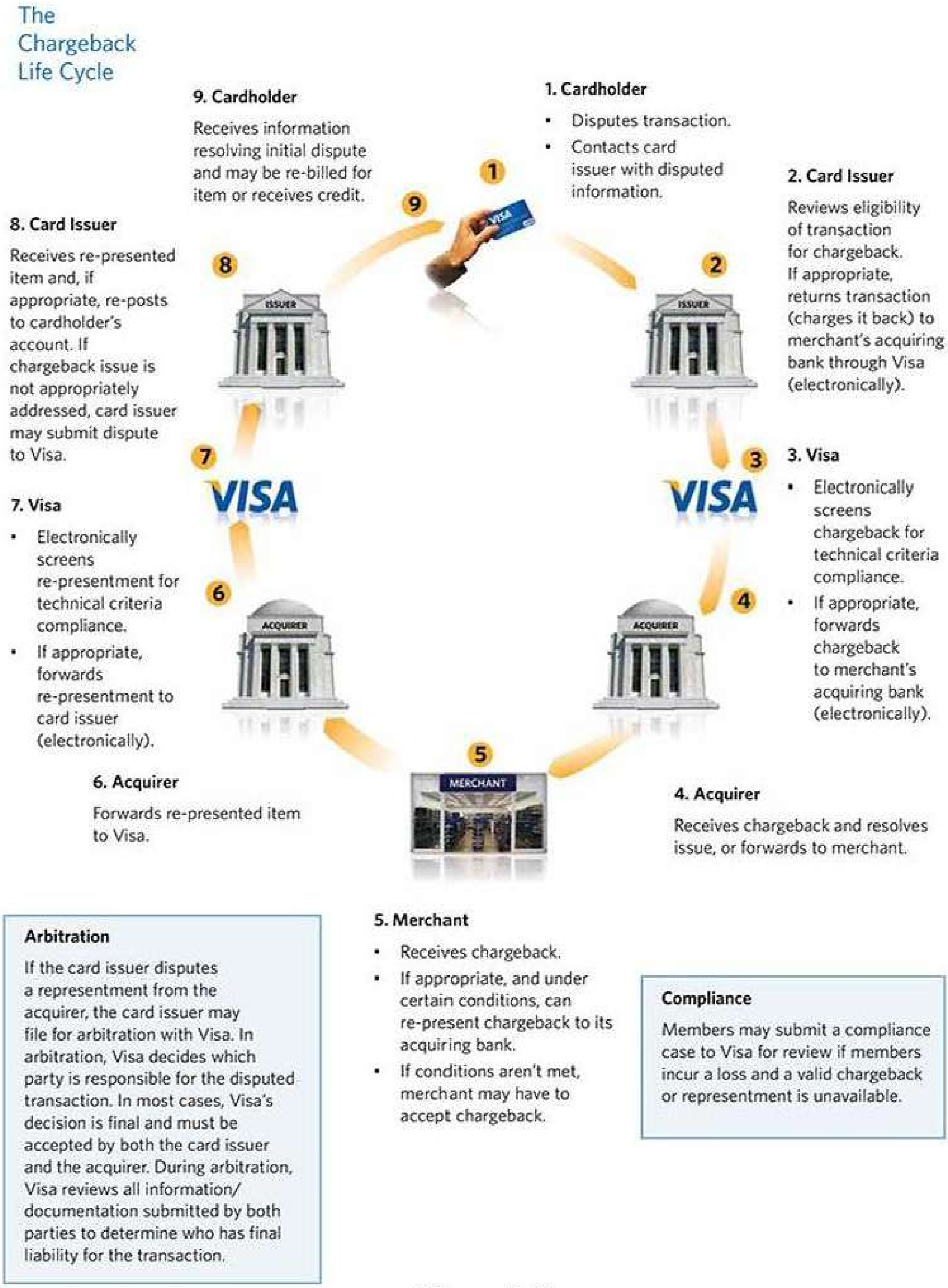


Figure 9.11: Chargeback functioning flow chart

Once the issuer receives this documentation, the first step is to determine whether a chargeback situation exists. There are many reasons for chargeback—those reasons that may be of assistance in an investigation include the following:

- Merchant failed to get an authorization.
- Merchant failed to obtain card imprint (electronic or manual).
- Merchant accepted an expired card when a chargeback right applies, the issuer sends the transaction back to the acquirer and charges back the dollar amount of the disputed sale.
- The acquirer then researches the transaction. If the chargeback is valid, the acquirer deducts the amount of the chargeback from the merchant account and informs the merchant. Under certain circumstances, a merchant may re-present the chargeback to its acquirer.

9.11 The Chargeback Life Cycle



The Chargeback Life Cycle

1. Cardholder

- Disputes transaction.
- Contacts card issuer with disputed information.

2. Card Issuer

Reviews eligibility of transaction for chargeback. If appropriate, returns transaction (charges it back) to merchant's acquiring bank through Visa (electronically).

3. Visa

- Electronically screens chargeback for technical criteria compliance.
- If appropriate, forwards chargeback to merchant's acquiring bank (electronically).

4. Acquirer

Receives chargeback and resolves issue, or forwards to merchant.

5. Merchant

- Receives chargeback.
- If appropriate, and under certain conditions, can re-present chargeback to its acquiring bank.
- If conditions aren't met, merchant may have to accept chargeback.

6. Acquirer

Forwards re-presented item to Visa.

7. Visa

- Electronically screens re-presentment for technical criteria compliance.
- If appropriate, forwards re-presentment to card issuer (electronically).

8. Card Issuer

Receives re-presented item and, if appropriate, re-posts to cardholder's account. If chargeback issue is not appropriately addressed, card issuer may submit dispute to Visa.

9. Cardholder

Receives information resolving initial dispute and may be re-billed for item or receives credit.

Arbitration

If the card issuer disputes a representment from the acquirer, the card issuer may file for arbitration with Visa. In arbitration, Visa decides which party is responsible for the disputed transaction. In most cases, Visa's decision is final and must be accepted by both the card issuer and the acquirer. During arbitration, Visa reviews all information/ documentation submitted by both parties to determine who has final liability for the transaction.

Compliance

Members may submit a compliance case to Visa for review if members incur a loss and a valid chargeback or representment is unavailable.

Figure 9.12

9.12 Best Practices for Safety

These suggestions will help you process card-not-present transactions securely and will substantially reduce customer disputes and fraud-related charge-backs.

1. **Educate and train your staff on e-commerce risk.** The extent of your risk exposure largely depends on your business policies, operational practices, the fraud detection and prevention tools you have implemented, security controls, and the types of products and services that you provide. Everyone in your organization should understand the risks associated with online transactions and be able to follow your established risk management procedures.
2. **Find the right payment processor.** The right credit card processing company will provide effective risk management support and help you understand the specific e-commerce fraud risk and liability. Adequate customer data protection capabilities are also something you will want to consider when making your selection.
3. **Create essential website content.** Your website must include and prominently display your privacy, shipping, return and refund policies. It must be reliable and to provide customers with easy and simple navigation. Placing links to these policies in the footer of your website will make them present on every page.
4. **Focus on risk reduction.** A well designed sales order process will help you address a number of risk concerns. You should indicate or highlight required transaction fields in your online payment acceptance form and verify card and card holder information that you receive from your customers over the Internet.
5. **Develop internal fraud prevention structure.** The profitability of your e-commerce organization depends on your internal strategies and controls for minimizing fraud. A risk management structure, combined with adequate transaction controls, will help you avoid fraud-related losses.
6. **Use fraud prevention tools.** There are a number of fraud prevention tools to help reduce your risk exposure. The most widely used among them are

the Address Verification Service (AVS), the Card Security Codes (CVV2, CVC 2 and CID), Verified by Visa and MasterCard SecureCode.

7. **Build a fraud screening process.** When adequately implemented, the screening of online card transactions can help you minimize fraud for large-ticket items and for high-risk transactions.

8. **Protect your merchant account from intrusion.** Implementing proactive measures can minimize the risk of criminals gaining access to your shopping cart or payment gateway and making fraudulent fund deposits.

9. **Participate in Verified by Visa and MasterCard Secure Code.** The two fraud prevention tools enhance security by requiring cardholders to authenticate themselves by entering a password during the checkout. The password is verified by the card issuer and, if correct, the transaction is allowed to be completed. Implementing Verified by Visa and MasterCard SecureCode protects merchants from fraud-related chargeback.

10. **Secure the process of routing your authorizations.** You must ensure that your authorization requests are submitted in a secure and efficient manner, before you can start accepting card payments over the Internet.

11. **Establish a process for handling transaction post-authorizations.** You need to set up an effective process for dealing with approved and declined authorizations before fulfilling an order.

12. **Ensure PCI compliance.** The Payment Card Industry (PCI) Data Security Standards (DSS) provide web-based merchants with standards, procedures and tools for protecting sensitive account information. You will need reliable encryption capabilities for data transmission and effective internal controls for protecting stored card and cardholder information. You will also need to review your security measures on a regular basis.

13. **Minimize unnecessary chargeback. Charge-backs** result in extra processing time and costs, while hurting your profits and may result in a loss of revenue. By carefully tracking and managing charge-backs, you will be able to set up concrete procedures for avoiding future charge-backs. You will also need to know your re-presentment rights.

14. **Monitor chargeback.** Effective chargeback monitoring mechanisms will help you detect excessive chargeback activity, identify the causes, and apply corrective measures to bring chargeback levels down. You can develop your own monitoring process or implement a third-party solution.

15. **Use collection efforts to minimize losses.** You can utilize a third-party collection service or build your own to help recover unwarranted chargeback losses.

9.13 Risks In E-Commerce Start Up

1. **Understand the risks and train your staff:**

   Your staff should know clearly what risks your e-commerce business may have to deal with. Everyone in your business structure needs to understand the types of risks inherent in online payments. Then, establish a procedure on avoiding and solving risks, which is a must for all staff to follow.

2. **Ensure information security:**

   Information here includes customer databases, buying requests, payment process etc. Internet is easily hacked by hackers so you need to ensure good security all the time to avoid data being changed or stolen. You need to set up a secure and efficient process for submitting authorization requests over the Internet, before you can start accepting card payments online.

3. **Select the right acquiring bank and merchant services provider:**

   The right acquiring bank and merchant services provide will provide effective risk management support have a complete understanding of e-commerce fraud risk and liability associated with online transactions. You will also want to consider an adequate customer data protection capability when making your selection.

4. **Create and display effective policies:**

   Your website must list your privacy, shipping, return and refund policies on each page. Customers should not be forced to search for them. This will also create satisfaction and convenience for customers to visit your page more often.

5. **Use collection efforts to minimize losses:**

You have control over most types of charge-backs and especially the ones resulting from processing errors. A well-designed collection system can help recover unwarranted charge back losses. So, all methods above are just some among a lot of methods to limit risks in e-commerce transactions.

9.14 Policies for Website Utilities

E-Commerce merchants communicate with their customers mainly through their websites. Moreover, a website is usually the first contact that a consumer makes with an e-Commerce merchant, further increasing its importance. If the first impression a potential customer gets is less than positive, the chances of him or her becoming a real customer will significantly decrease. Beyond the marketing side of your website there are certain requirements that e-Commerce merchants have to comply with. In order to avoid customer disputes or misunderstandings, you must develop a privacy policy which needs to incorporate the following best practices:

1) **Make it Clear and Concise.** You will want your customers to understand their responsibilities, as well as yours so your privacy statement should be concise and readable. It may also be subject to legal requirements and you will have to consult with an attorney about it. Typically, to address consumer concerns about providing personal data, your privacy policy should provide details on:

- What customer data is collected and tracked.
- Whether this information is shared with third parties and, if so, with whom.
- How customers can opt out.

2) **Make it Available to Visitors through a Link on your Homepage.** Your website's homepage is usually the most trafficked page and your Privacy Policy should be made available there. It is a good idea that you place a link to it in your website's footer or header which typically remains the same on all of your pages so that visitors will have a ready access from anywhere.

3) **Register with a Privacy Organization.** A good way to enhance your website's security credentials is to register with a privacy organization and obtain a "seal of approval" or an equivalent from them.

9.15 Self Learning Exercise

Q.1 Kerberos is an encryption-based system that uses

a) Secret key encryption

b) Public key encryption

c) Private key encryption

d) Data key encryption

Q.2 The method(s) of payment for online consumers are

a) Electronic cash

b) Credit/debit

c) Electronic checks

d) All of the above

Q.3 E-Commerce is not suitable for

a) Sale/Purchase of expensive jeweler and antiques.

b) Sale/Purchase of mobile phones.

c) Sale/Purchase of branded clothes.

d) Online job searching

Q.4 Telnet is a

a) Network of Telephones

b) Television Network

c) Remote Login

d) Remote Login.

Q.5 The internet is

a) Network of networks

b) Web site.

c) Host

d) Server

9.16 Summary

Risk management is relevant to all organizations (public and private, large or small). It should be a part of the culture of the organization, with a pro-gramme and an effective policy led by top management with transparent responsibilities laid down for every manager and employee to be involved in the management of risk.

9.17 Glossary

Encrypt: Convert (information or data) into a code, especially to prevent unauthorized access.

AVS : Address Verification Service

9.18 Answers to Self Learning Exercise

Q.1 (a)

Q.2 (d)

Q.3 (d)

Q.4 (c)

Q.5 (a)

9.19 Exercise

Q.1 What is Risk Management? Discuss with example.

Q.2 Define best practices for safety?

Q.3 Explain chargeback life cycle.

Q.4 What role does Internet in any business?

Q.5 Discuss data and payment gateway security.

References and Suggested Readings

1. Essentials of risk Management by Michel Crouhy, Dan Galai, Robert Mark.
2. The practical guide for Risk Management by Thomas s. Coleman.
3. Financial Risk Management: A Practitioner's Guide to Managing Market and Credit Risk by Steve L. Allen.

UNIT-10

Electronic Data Interchange

Structure of the Unit

10.0 Objective

Main Objectives are :

- This unit focuses how business documents are exchanged / transferred between counterparts through the intermediary without or less human inputs.
- The main objective of EDI is to replace paper documents by electronic document flow between information systems. With the help of this material, students will aware how electronically documents are exchanged and used for purpose.
- In addition to it, they will also know the legal requirements required in e-commerce business.

10.1 Introduction

EDI stands for Electronic Data Interchange which provides an electronic way of transferring business documents in an organization internally between its various departments or externally with suppliers, customers or any subsidiaries etc. In EDI, hard copy of documents are replaced with electronic documents like word documents, spreadsheets etc. Simple example of EDI is to replace the traditional postal via fax and email i.e., email is an electronic approach for documents to transfer to an individual or many people with the help of computers.

Electronic data interchange (EDI) provides a common platform to electronically exchange of business documents between organizations. The main goals of EDIare:

- To remove the paper work environment by replacing information electronically
- To normalize and combine data
- To integrate data processing in Information System.
- To reduce the manual labour
- To increase speed and accuracy of data collection
- To guarantee efficient delivery of data
- To provide necessary control, management and authorization of information flows
- To guarantee information security

10.2 EDI Definition

Electronic Data Interchange (EDI) is computer based transmission of business documents in a standard electronic format followed by some standards and regulations.

EDI documents can be exchanged through with the use of appropriate application on the source and receiver's computer (e.g., the Order Management System) and processing can begin immediately. A typical manual system looks like the following process flow having lots of paper and people shown in the following figure:

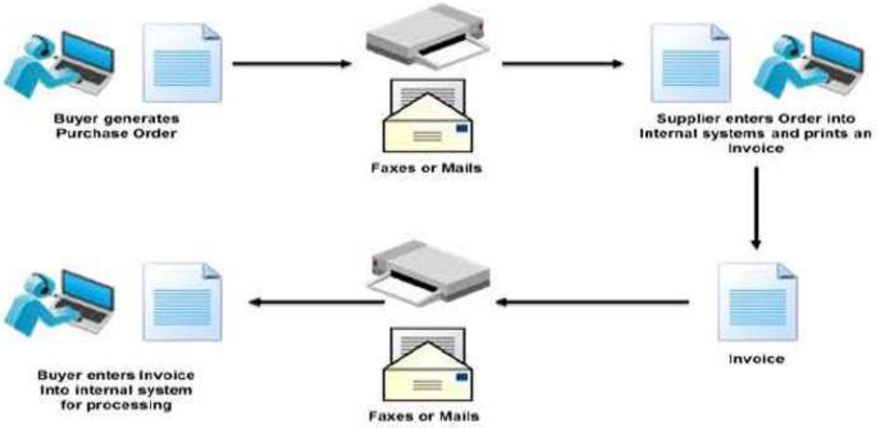

Buyer generates Purchase Order
Faxes or Mails
Supplier enters Order into internal systems and prints an invoice
Invoice
Buyer enters Invoice into internal system for processing
Faxes or Mails

Figure 10.1: Traditional process

The EDI process looks like below where main advantages are no paper and less number of people involved:

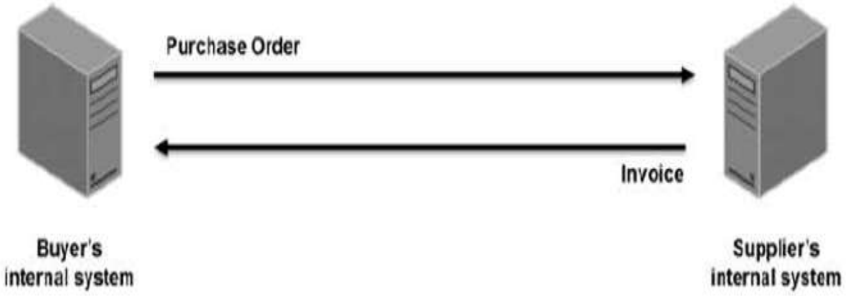


Figure 10.2: EDI process

10.3 Benefits of EDI

There are several benefits of using EDI applications. But, the major benefits of EDI mainly focused on the criteria like- cost-saving, speed and accuracy, efficiency and business strategies. These are described below:

Cost saving benefits of EDI:

- The cost saving benefits includes reducing the expenses related to the paper such as-printing, reproduction; storing, packaging and data retrieval while using the EDI based applications.
- EDI also reduces the manufacturing cost.

- It also focus to the elimination of errors generated during the illegible faxes, lost orders or incorrectly taken phone orders and also saving staff valuable time.

Speed and Accuracy benefits of EDI:

- EDI transfer of our information within a second instead of waiting from the postal service. So, it speeds up business rate high and provides many business opportunities.
- It also cares about the data quality and its improvement. It also reduced the delivery of transactions by reducing errors from obscured writing, failing delivery of faxes/mail errors.
- EDI also helpful to reduce the order-to-cash time which improves the business relationships.

Efficiency related benefits of EDI:

- EDI application increases the productivity of staff/s on concentrating the tasks.
- It provides quick processing of accurate business documents.
- It provides automated data transfer in a supply chain process which guarantees for the integrity and on time delivery and tracking in real time of business-critical data.
- It takes less time to the order processing and delivery of the order.

Strategies based benefits of EDI:

- It provides real-time visible transactional status of the document. It also allows demand-driven business model rather than a supply-driven.
- It provides a new business markets by product enhancements and new product delivery.
- EDI helps to bring business world come closer.
- It also maintains and promotes corporate social responsibility.

10.4 Shortened Ordering Time

As EDI focus to the electronic exchange business process where documents are delivered in less amount of time by maintaining the quality of it. The order placing in traditional manner takes too much time whereas in EDI, it is placed in a very short amount of time. During the placing of order, EDI application maintains the privacy and quality of order. Concern receiver gets the order by the concerned sender. However, maintaining the ordering time by using the EDI application/s, it also reduce the lots of efforts, manpower and saves our valuable time and most importantly, it gives the new business opportunities and establishing the business relationship nationally as well as geographically.

10.5 EDI Example

There are lots of examples of EDI. Almost all company, institutes are turned to EDI application. Govt. of India is also promoting the electronic exchange with Gem Portal- an e-market place and moving on this direction because of its huge benefits. Today, we are purchasing of goods or product/s online through various e-commerce applications such as- Amazon.com, paytm.com etc. All these follow the EDI process.

Example-1

Below is an example to understand the business transactions/documents where many different companies share the documents.

- Purchase order (PO)
- Sales order(SO)
- Invoice
- Advance Ship Notice (ASN)
- Functional Acknowledgement

Each company maintains the document in a specific format to send the documents. Consider there are two companies A and B. Company A sends its purchase order (PO) to company B. Since, company A has different format for the document to the Company B format, so it will manually read the data from PO sent by Company A and creates a Sales order (SO) from it in order to carry out further processes. Here, EDI maintains the data exchange format by providing a common Data exchange format which reduces the manual intrusion during the process. The following figure gives a basic understanding of the process of EDI.

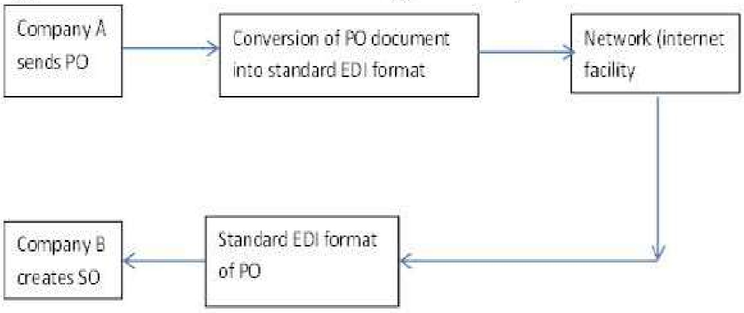

Company A sends PO
Conversion of PO document into standard EDI format
Network (internet facility
Standard EDI format of PO
Company B creates SO

Figure 10.3 : Process of EDI

EDI provides process of transaction speedily and increase the accuracy to the information being sent from one business to another. By using EDI based applications, everything is fully automated and smooth with less human intervention.

In addition to it, in the above example, EDI may allow to Company A to select the vendors, plan the production schedules electronically and create purchase order (PO) automatically. The errors involved here are minimal as there is less human involvement. When the PO reached at Company B end, the EDI helps to create Sales order (SO) automatically without any human involvement of creating Sales Order from PO sent by Company A.

The most preferable network is used in EDI process is Value added networks. This is the third party network that provides services to execute authorized transactions with valid trading partners using EDI. Each VAN has a centralized computer system that maintains the files for each user.

Standardized EDI format:

Different organizations use different format. In this connection, EDI provides a common format for different purpose. There are some examples of EDI standard format used by different organizations-

- **UN/EDIFACT standard**

  It is basically used for administration, Commerce and Transport. It is developed under UNITED NATIONS (UN) in 1987.

- **ANSI ASC X12**

It is used by health care, insurance, government and transportation. It is employed by American National Standards Institute (ANSI) in 1979.

- **GS1 EDI**

  It is used by Supply chain process for carrying out processes like Order, Dispatch Advice (Shipping Notice), Invoice, Transport Instruction, etc.

- **TRADACOMS**

  It is used by UK retail sector. It contains transaction like Product information file, Price information file, the customer Information file, the order file and many more operations.

- **HL7**

  It provides standard format for exchange of information related with retrieval of electronic health information.

Example-2

Suppose a XYZ manufacturing company manufactured the products A and B. This company reviews the sales and orders at the end of month, making prediction of the sales for the next month. Sales estimation is matched to the available raw material stocks and other components. Based on this, a production plan is formed. The monthly plan requires being flexible so that products could be well-ordered in a short amount of time if there is no availablability of product/s in the store. Here, packing product should only be placed for just in time (JIT) delivery, so that product A can cut down from the stock of packaging which reduce the inventory cost. On the other hand, packaging supplier also wants to improve its processing of orders, particularly urgent orders.

Both products A & B and its supplier start using EDI system, any change of the plan (i.e. schedule) on the production control system will review the product materials requirements and the order is automatically created. The order generated using EDI application, each placed order and its product information is well stored and coded and also framed in structured and accepted format.

10.6 Legal Requirements in E-Commerce

Almost each and every country worldwide has specific rules, regulations and laws for EDI based e-commerce application. The main focus of legal rules, regulations and laws for EDI is to the presentation, process of work and contents in the website that govern the websites.

So, the setting up of a successful e-commerce business is not only concerned but there are many issues that must be needed and considerable to establish an e-commerce business making it successful. The legal issues focus to brand promotion and protection also. In addition to it, domain name protection policy is a vital part of making e-commerce project successful.

Traditional legal systems have a great difficulty in keeping pace with rapid growth of the Internet and its impact throughout the world. Growth of e-commerce gave rise to a variety of legal issues, which is related to intellectual property rights, copyright, trademark, privacy etc. Cyber law governs the legal issues of cyberspace. The term cyberspace is not restricted to the Internet. It is a very wide term that includes computers, computer networks, the Internet, data software etc. E-commerce is one of the most cost-effective business models in India these days and e-commerce markets are getting increased day by day. Not only its current growth is good but its future and projected growth is tremendous. However, e-commerce in India, legal issues are considerable.

E-commerce websites functioning in India are required to follow many laws of India including the Information Technology Act, 2000 (IT Act 2000, amendment 2008). As per the IT Act, 2000, the e-commerce websites operating in India are Internet intermediaries and they are required to fulfil and obey cyber law due persistence requirements as well.

E-commerce in India involves some agreements with other laws such as- contract law, Indian penal code, etc. However, some compliance is also necessary in online shopping in India with banks and financial norms are required in India. For example, consider the PayPal online system for payment. It is a kind of soft money. If PayPal allows online transaction of its receipt and disbursements for its existing or proposed e-commerce activities then in this situation, it is required to take a license from Reserve Bank of India (RBI). More than this, other online payment transferors in India is also applied to be perceived.

As electronic commerce in India is active, the dispute resolution of electronic commerce in India is also essential to be strengthened. The existing litigation system in India is not encouraging the development of e-commerce in India but online disagreement resolution in India is more suitable for such purposes.

However, those who are providing, engaging and using cloud computing, virtualization and other Internet based e-commerce services in India; they must follow the techno legal regulations of India. Cloud computing legal and regulatory requirements in India for businesses and entrepreneurs are still growing. Even they must obey the cloud computing business community of India. More importantly, encryption laws and cyber law due diligence in India must be ensured by those who are providing the Virtualization and cloud computing service in India.

We can conclude here that, the cost-effective e-commerce in India must be discovered only after fulfilling with the laws governing by the respective e-commerce segment. There are multiple set of laws and regulations in India that manage all e-commerce segments where every e-commerce segment is governed by different laws.

There are some legal issues, described below which must be considerable and required for every e-commerce business:

Data Protection :

User Data protection is a very crucial part for any e-commerce business. So it must be closely consideration.

- First of all we need to register under the Data Protection Act for collecting any kind of details from customers, employees or potential customers etc. The details may include names, addresses, telephone numbers and email addresses.
- Secondly, we have to Cleary state what we do and what we intend to do.
- The Act may be applied to any size of business.
- Export and Import of individual information is not allowed without his/ her permission.

- Security of data is very important, it must be properly maintained and it must be exposed or removed based on the user request and from the subjects of the information.

For further details of the act you should consider: The Data Protection Act 1998

Consumer Protection (Distance Selling) Regulations:

The Consumer Protection (Distance Selling) Regulations 2000 is also an important act which is considerable and it applies to many e-commerce websites. However, this act is not applicable on ‘business-to-business' transactions. According to this act, you must

- Clear indicate the products and services before selling of the product.
- Clear mentioning of postage and packing costs, considering the VAT or any other taxes, properly included in the prices on the website.
- There must be a written confirmation of order following purchase, for example a confirmation email.
- Cooling off period features must be included where customer can update or cancel the order or return the order.
- It must be clearly inform to customers of their right to cancel their order with no loss other than return postage and packing.

For further information about the act, please see: The Consumer Protection (Distance Selling) Regulations 2000

E-commerce Directive or Instructions:

- It is mandatory that each organizations must mention what kind of business they are doing (i.e. name of business), registration number of company including proprietor's name, location, contact information (i.e. telephone number and email address), VAT registration number (if registered) etc.
- You may refer to trade or professional schemes if applicable.
- Mention the information on price, tax and delivery to buyers.
- There must be Terms and Conditions which must be mention clearly.
- You must acknowledge all orders.

- Communication with customers anytime there must be electronic communication designed of the company that promotes goods or services.
- Sender of all electronic communication must be clearly mentioned.
- Promotional offers must be acknowledge to the customer time to time.

For more information, you should see for further details of this regulation: The Electronic Commerce (EC Directive) Regulations 2002

E-privacy directive (ICO Cookie Law):

This law is also a very important in e-commerce world. The law deals with the packing, procuring and storing access of information of visitors on the website.

- Information regarding the storage of, or access to that information must be clearly stated on the website
- There must be clear and proper information available on the use of cookies acknowledged to visitors on the website.
- Cookies used for functional purposes do not need for permission.

10.7 Limitations of EDI

The big limitation of any EDI based application that it requires Internet facility to proper exchange of information because EDI application is based on the internet. But there are also other limitations of EDI which may discourage to any e-commerce business. Fewer are described below:

- As we know that one of main task of EDI to provide a common standard format among different companies format. Sometimes, setup and maintenance of formats are very expensive.
- Starting a new e-commerce business is a very crucial part, so initial setup is time consuming.
- Cost is also important factor in e-commerce application. Thus, cost at initial level to setup EDI may discourage.
- Nowadays, EDI spreads their foot on almost every business process and business process are getting depend on EDI standard format. If any of the

standard format changes then the business process has to be changed accordingly. So this is also a big limitation.

- As user data is crucial so the protection of it from viruses, hacking, malware and other frauds are also important concerns.
- EDI based application requires some training to the staffs in order to implement and running EDI application/s before launching it.
- Proper backup should be maintained as the whole data depends on EDI. In case of any crash of EDI system, proper backup has to be maintained and extra cost is required for it.
- Some company stops doing business and not uses EDI. This makes the market limited.

10.8 Self Learning Exercise

Q.1 Explain EDI.

Q.2 Write advantages and disadvantes of EDI.

Q.3 What is E- Commerce?

10.9 Summary

Electronic data interchange (EDI) is one of the most mutual methods of organized exchange of business documents between organizations by electronic means. It helps to decrease the load of manual transaction process. This improves the productivity of the human and in work cultural environment.Many bigfirms or business organizations are adopting the EDI-based solutions (with its many benefits) to associate with their business associates or companies. E-commerce is one of the EDI applications. Before using EDI based application or services, some legal issues (such as- rules, regulation and acts) are carefully keep intend and need to understand it.

10.10 Glossary

Purchase order (PO): is a commercial document between a buyer and a seller. It is basically the first official offer issued by buyer related to the products or services including its types, quantities, and agreed prices are indicated. It is used to control the buying of products and services from external suppliers.

Sales order (SO): is a documentdeal out by a business or sole trader to a customer.

Invoice: It is a document generated by seller that is for a buyer in which amount and cost of products or services are specified.

Advanced shipping notice (ASN): is a document that provides detailed information related to a pending delivery.

Functional Acknowledgement: It is an EDI document or more accurately says an electronic receipt which is a kind of acknowledgement, sent to inform a trading partner of a purchase order for its accepting or processing. 997 Functional Acknowledgments are used to indicate to a trading partner.

10.11 Exercise

Q.1 Explain the importance and challenges of E- Commerce.

Q.2 Describe the legal and ethical issues in E-commerce

References and Suggested Readings

1. Web Commerce Technology Handbook, Minoli et al, McGraw Hill
2. Internet Commerce: Digital Models for Business, Lawrence et al, Wiley
3. Designing Systems for Electronic Commerce, Treese et al, Addison-Wesley
4. https://en.wikipedia.org/wiki/Electronic_data_interchange

UNIT-11
Electronic Payment Machine

Structure of the Unit

11.0 Objective

The Issues of trust and protected business communication play a significant role in the e-commerce world than in conventional business as far as payment systems are concerned. Traditional responsibility of e-commerce, a customer sees a product, examines it, and then pays for it by cash, cheque, or card. In the e-commerce, in most belongings the customer does not truly see the physical product at the time of transaction and technique of payment is performed electronically. EPSs facilitate a customer to pay for the goods and services online by using incorporated hardware and software systems.

Figure11.1: EPS System facilities

The main objectives of EPS are to boost efficiency, improve security, and develop customer convenience and simplicity of use for better services. Although these systems are in their irresponsibility, some major development has been made for ease of use. There are several methods and tools that can be used to enable EPS implementation.

11.1 Introduction

An **EPS** facilitates the recognition of electronic payment for online transactions. Also known as Electronic Data Interchange (EDI), **EPS** have become ever more popular due to the widespread use of the Internet-based shopping and banking services. It would be difficult for an online retailer to work without sustaining credit and debit cards due to their extensive use for Internet-based shopping and banking services. Increased security events include use of the card verification number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank.

Also online merchants have to fulfill with harsh rules predetermined by the credit and debit card issuers (Visa and MasterCard) this means that merchants must have security protocol and dealings in place to ensure transactions are more protected. This can also consist of having a certificate from an authorized certification authority (CA) who provides PKI (Public-Key infrastructure) for securing credit and debit card transactions.

In the interim, the use of smart cards has become very popular. A Smart card is like to a credit card; yet it contains an embedded 8-bit microprocessor and uses e-cash which transfers from the consumers' card to the sellers' device.

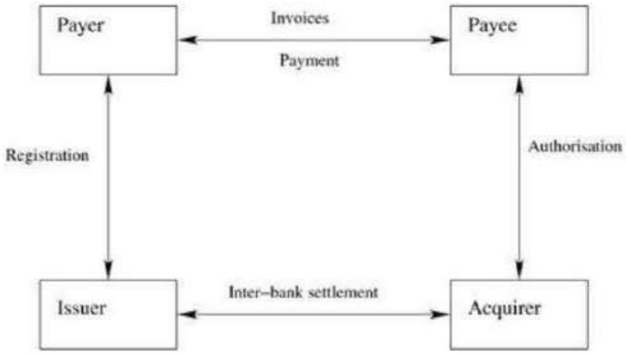


Figure11.2: EPS Processing flow diagram

A popular smart card initiative is the VISA Smart card. Using the VISA Smart card you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the Internet.

11.2 Electronic Payment System (EPS)

An **e-commerce payment system** facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the Internet-based shopping and banking. Credit cards have become one of the most common forms of payment for e-commerce transactions. Increased security measures include use of the Card Verification Number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank. Also online merchants have to comply with stringent rules stipulated by the credit and debit card issuers (Visa and MasterCard) this means that merchants must have security protocol and procedures in place to ensure transactions are more secure.

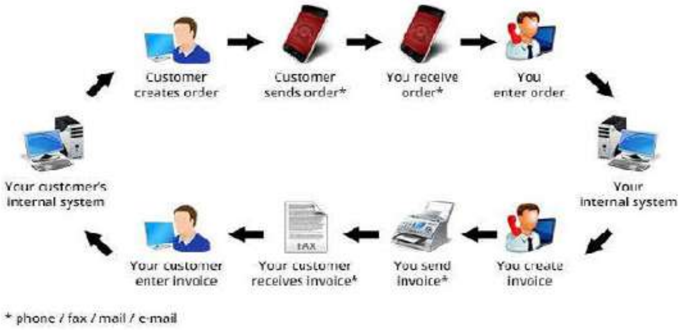


Figure11.3: Customer's internal system

A well-liked smartcard proposal is the VISA Smartcard. Using the VISA Smartcard customer can transfer electronic cash to their card from their bank account, and customer can then use their card at various retailers and on the Internet.

Figure11.4: Smart Cards of Various companies

There are many companies that allow financial transactions to acquire over the Internet, such as PayPal. The pace and cleanness with which cyber-mediary accounts can be recognized and used have contributed to their extensive use, although the risk of violence, theft and other harms with discontented users often accusing the mediaries themselves of unfair performance is associated with them.

Methods of online payment:

Credit cards comprise an admired method of online payment but can be costly for the merchant to accept because of transaction fees primarily.

Debit cards invent an excellent substitute with similar security but usually much cheaper charges.

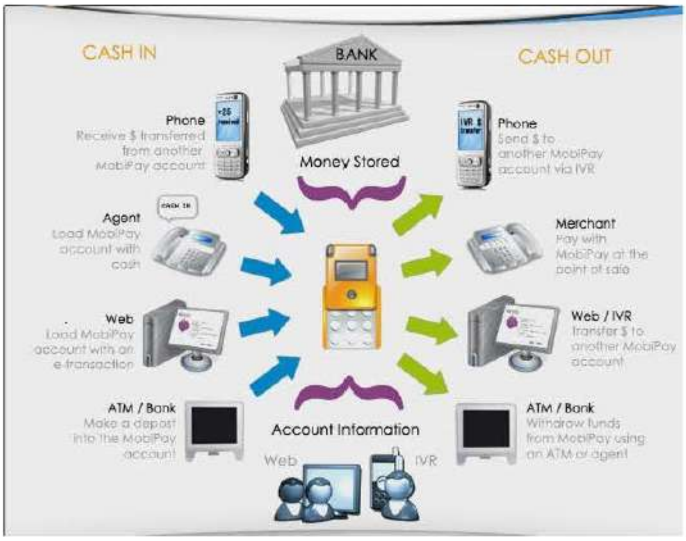

CASH IN
BANK
CASH OUT
Phone
Receive $ transferred from another MobiPay account
Money Stored
Phone
Send $ to another MobiPay account via IVR
Agent
Load MobiPay account with cash
CASH IN
Merchant
Pay with MobiPay at the point of sale
Web
Load MobiPay account with an e-transaction
Web / IVR
Transfer $ to another MobiPay account
ATM / Bank
Make a depost into the MobiPay account
Account Information
ATM / Bank
Withdraw funds from MobiPay using an ATM or agent
Web
IVR

Figure11.5: Mobile Pay system flow chart

11.2.1 Net Banking :

This is a scheme, well known in India which does not engage any type of physical card. It is used by customers who have financial records enabled with Internet banking. Instead of entering card details on the purchaser's site, in this system the payment gateway allows one to specify which bank they wish to pay from. Then the user is redirected to the bank's website, where one can validate oneself and then approve the payment. Naturally there will also be some form of two-factor authentication.

11.2.2 PayPal :

PayPal is a worldwide e-commerce business allowing payments and money transfers to be made through the Internet. Online money transfers provide as electronic alternatives to paying with traditional paper methods, such as cheques and money orders. The amount depend on the currency used, the payment alternative used, the country of the sender, the nation of the recipient, the amount sent and the recipient's account type. In count, e-Bay purchases made by credit card through PayPal may acquire extra fees if the buyer and seller use different currencies.

Figure11.6: Paypal system with eligible card scheme

11.2.3 Paymentwall:

An e-commerce solutions providing company launched in 2010, offers a broad range of online payment methods that its clients can incorporate on their website.

Figure11.7: Mobile Paymentwall system mobile application image

11.2.4 Google Wallet:

Google Wallet was launched in 2011, serving similar function as PayPal to ease payments and transfer money online. It also features a security that has not been cracked to date, and the ability to send payments as attachments via email.

11.2.5Mobile Money Wallets:

Telecom operators have started offering mobile money wallets which allows totaling of funds easily through their obtainable mobile subscription number, by visiting substantial recharge points close to their homes and offices and converting their cash into mobile wallet money. This can be used for online transaction and e-commerce purchases.

11.3 Electronic Fund Transfer (EFT)

Electronic funds transfer (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, through computer-based systems and without the direct interference of bank staff. In the other countries, they may be referred to as electronic cheques or e-cheques.

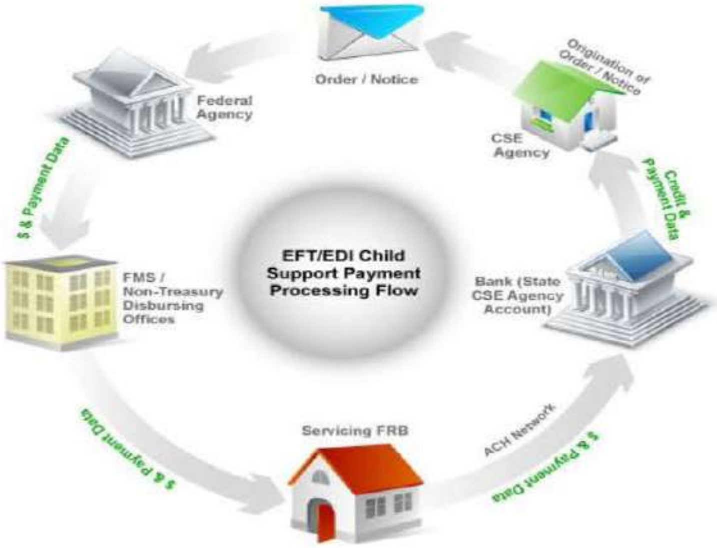

Order / Notice
Origination of Order / Notice
Federal Agency
CSE Agency
$ & Payment Data
Credit & Payment Data
EFT/EDI Child Support Payment Processing Flow
FMS / Non-Treasury Disbursing Offices
Bank (State CSE Agency Account)
$ & Payment Data
Servicing FRB
ACH Network
$ & Payment Data

Figure11.8: Diagram of EFT Payment procedures

The term covers a number of different payment systems, for example:

- Cardholder initiated payment transactions, using a payment card such as a credit or debit card.
- Direct deposit payment or cash amount initiated by the payer.
- Direct debit payments for which a business debits the consumer's bank accounts for payment services. Wire transfer via an international banking network.
- Electronic bill payment facility in online banking, which may be delivered by EFT or paper cheque.
- Transactions involving stored value of electronic money schemes, possibly in a private currency.

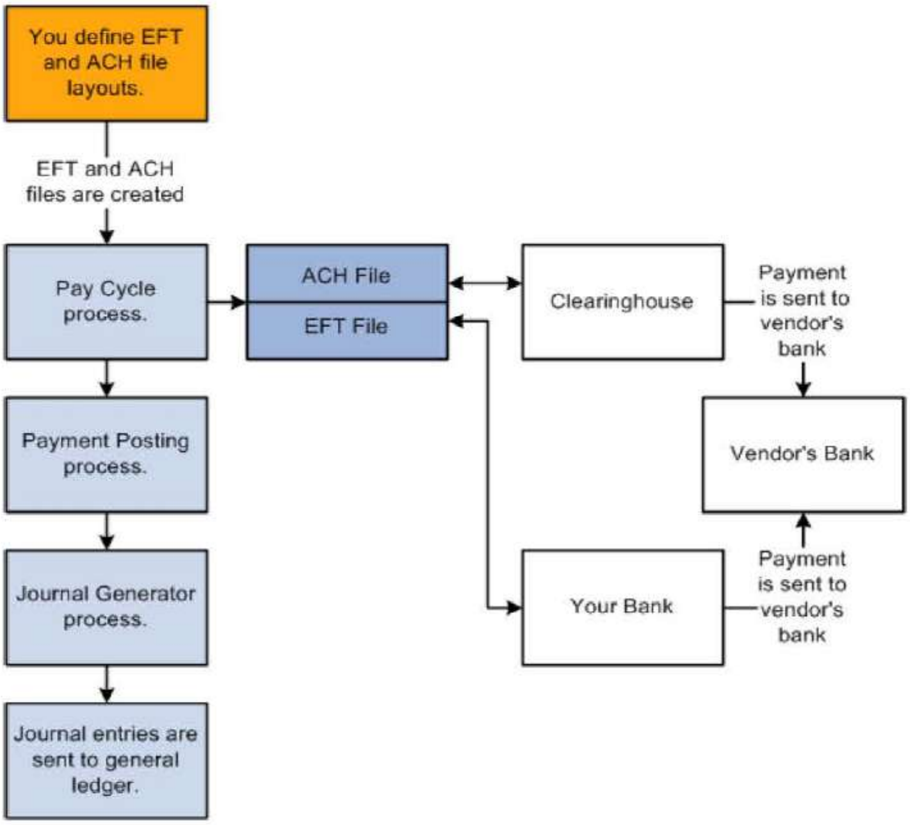

You define EFT and ACH file layouts.
EFT and ACH files are created
Pay Cycle process.
ACH File
EFT File
Clearinghouse
Payment is sent to vendor's bank
Vendor's Bank
Payment Posting process.
Journal Generator process.
Your Bank
Payment is sent to vendor's bank
Journal entries are sent to general ledger.

Figure11.9: Flow chart of EFT

11.4 Payment Cards

A payment card is a device that enables its owner (the cardholder) to make an expense by electronic funds transfer. The most ordinary types of payment cards are credit cards and debit cards. Payment cards are regularly imprinted plastic cards, 85.60 × 53.98mm in size, which comply with the ISO/IEC 7810 ID-1 standard. They usually also have printed card number conforming to the ISO/IEC 7812 number standard.

Figure11.10: Payment card

Most usually, a payment card is electronically associated or linked to an account or accounts belonging to the cardholder. These accounts may be deposit or drop accounts or loan or credit accounts, and the card is a means of authenticating the related cardholder. On the other hand, stored-value cards are cards that accumulate money on the card itself.

11.4.1 Credit Card:

The issuer of a credit card creates a manifestation of credit (usually called a credit limit) for the cardholder on which the cardholder can sketch (i.e. sponge), either for payment to a commercial for a purchase or as a cash move ahead to the cardholder. Mostly credit cards are issued by or through confined banks or credit unions, but some non-bank economic institutions also propose cards explicitly to the municipal. The cardholder can choose either to repay the full outstanding balance by the payment due date or to pay back a minor amount, not less than the "minimum amount", by that date.

11.4.2 Debit Card:

With a debit card (also known as a *bank card*, *cheque card* or some other explanation) when a cardholder makes a purchase, funds are kept directly either from the cardholder's bank account, or from the left behind balance on the card, instead of the holder reimburse the money at a afterward date. In a number of cases, the "cards" are designed completely for use on the Internet, and so there is nothing like material card. Like credit cards, debit cards are used widely for telephone and Internet purchases.

Debit cards can also allow instant withdrawal of cash, provisional as the ATM card, and as a cheque assurance card. Merchants can also opinion "cashback"/"cashout" facilities to customers, where a customer can withdraw cash along with their acquisition. Merchants usually do not assert a fee for purchases by debit card.

11.4.3 Charge Card:

With charge cards, the cardholder is essential to pay the occupied balance shown on the account, which is frequently issued monthly, by the payment due date. It is a form of short-range loan to bind the cardholder's purchases, from the date of the purchase and the expense due date, which may typically be up to 55 days. If payment is not made in complete, this may outcome in a late payment fee, the possible limit of future transactions, and maybe the termination of the card and refund back within 24 hours.

11.4.4 ATM Card:

An ATM card is any card that can be used in automated teller machines (ATMs) for dealings such as deposits, cash withdrawals, obtaining account information, and other types of transactions, customarily through interbank networks. Cards may be issued entirely to access ATMs and mainly debit or credit cards may also be used at ATMs, but charge and proprietary cards cannot.

11.5 Electronic Cash (E-Cash)

The key function of e-cash is to assist transactions on the Internet. Several of these transactions may be small in size and would not be cost well-organized through other payment mediums such as credit cards. These types of payments, revolving the Internet into a transaction oriented forum, involve mediums that are trouble-free, low-priced (from a merchants perspective), private, and secure. Electronic Cash is the ordinary solution, and the companies that are revolutionary these services shape that the products will assemble the stated criteria. By providing this type of payment instrument, the incentives to provide meaningful services and products via the Internet should enlarge. Another forthcoming beneficiary from these developments would be Shareware providers, since presently they not often receive payments. To whole the digital money revolution an offline design is also required for the pocket money/change that most people must hold for small transactions (e.g. buying a newspaper, buying a cup of coffee, etc...).

The banks utilize electronic fund transfer. Electronic money, removes the middleman. Instead of requesting the banks to transfer the funds from side to side the mechanism of a cheque, the E-cash user only transfers the money from his bank account to the account of the receiver.

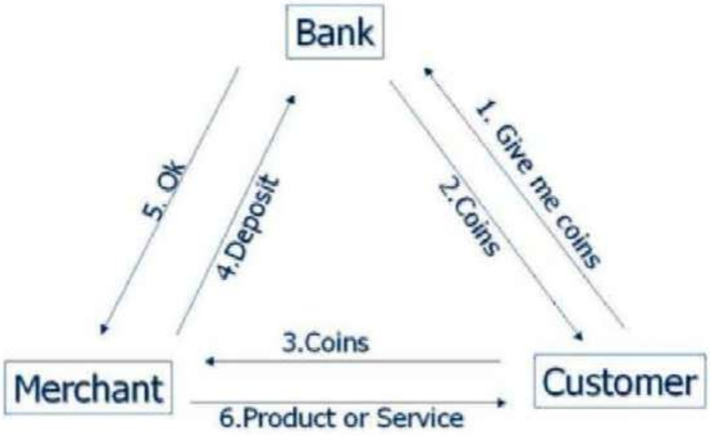


Figure11.11: E-Cash Flow Chart for functioning

The truth of E-cash is only to some extent more complicated, and these complications make the transactions both secure and concealed. The user downloads electronic money from his bank account using extraordinary software and stores the E-cash on his local hard drive. To pay a WWW merchant electronically, the E-cash user goes through the software to pay the desired amount from the E-cash "wallet" to the merchant's neighboring hard drive ("wallet") after passing the transaction through an E-cash bank for authenticity confirmation. The merchant can then shell out its bills/payroll with this E-cash or upload it to the merchant's hard money bank account. The E-cash company makes money on each deal from the merchant and from royalties paid by banks which make available customers with E-cash software/hardware for a small monthly fee. Transactions between individuals would not be issue to a fee.

E-cash truly globalizes the economy, since the user can download money into his cyber-wallet in any currency desired. A merchant can admit any currency and translate it to local currency when the cybercash is uploaded to the bank account.

To the quantity a user wants E-cash off-line all that is essential about smart card technology. The money is loaded onto the smartcard, and particular electronic wallets are used to offload the money onto additional smartcards or directly to an on-line system. Smartcards have been used unbeaten in other countries for such transactions as phone calls for a number of years. The money could also be detached from a smartcard and returned to a bank account. Visa is developing a connected product, the stored value card. This card comes in a diversity of denominations, but functions more similar to a debit card than E-cash.

11.6 Electronic Cheques (E-Cheques)

When a person wrote a personal checque to make a buy, the recipient delivered it to their bank for deposit and it was processed physically. It was a method that could take days to complete, which meant the depositor had to stay for the funds to clear.

Today, new technology has reduce a lot of the time of banking work and attempt of the past by turning a paper cheque into an electronic transfer (debit), also known as an electronic cheque or e- cheque. A merchant or service provider can electronically transfer funds from a customer or client's bank account directly into their bank account through the Federal Reserve Bank's Automated Clearing House (ACH) system.

Electronic cheque payment processing is cheque cashing basic, a stress-free and inexpensive way to get paid quicker. It is also just one of the many important merchant services that TransFirst provides to its clients to meet all their payment processing needs, including credit cards and debit cards.

E- cheque Process:

The e-cheque route begins when a customer writes a paper cheque at the point of sale. The clerk runs the cheque through a reader or imager that captures the necessary information, including cheque number, account number and number identifying the financial institution (routing number). The clerk enters additional merchant-related information to complete the one-time electronic payment from the designated account. Depending on the merchant's concurrence with their payment processor, the cheque is verified or guaranteed by the provider. A receipt is generated and printed for the cheque writer to sign; the cheque is voided and returned to them.

11.7 Electronic Wallets (E-Wallets)

The transaction will show on the customer's bank statement as a debit, not a cheque. The merchant uploads the captured cheque information to their payment supplier for processing, and the proceeds are deposited into the merchant's account within 1 to 2 business days. The process is alike for a cheque that is mailed in payment of a bill, except the cheque is retained by the merchant after it is voided.

"Wallet" in the straight sense of the term, refers to a purse or folding case for securely holding money or personal information such as identity card. Digital or Electronic Wallet (e-wallet) refers to an electronic, Internet based *payment system* which stores financial value as well as personal identity linked information. Such electronic payment systems facilitate a customer to pay online for the goods and services, including transferring funds to others, by using an incorporated hardware and software system. Hardware can be a device like mobile or computer. Communication between the buyer and the seller may happen over the internet or blue tooth or on mobile set of connections. Thus, e-wallet is nothing but an online money account which does not oblige the use of a corporal card for undertaking transactions/remittances. Unlike savings bank accounts, they, at present, do not tender any interest for keeping money in it, but rewards the holders in the course of cash-backs for making purchases through it. Contrasting credit cards, e-wallets are preloaded money. Therefore it resembles more to a debit card.

E-wallet is a part of the payment system. The expression "payment system" is defined in India to mean a scheme that enables payment to be effected between a payer and a beneficiary, involving clearing(in which the payment service provider acts as a counter party between the buyer and seller by calculating the obligations among them and guaranteeing its settlement), **payment** (act of paying or transacting) or **settlement service** (the final act of changing the records of ownership of the advantage transacted, either after netting all the fractious obligations or on gross terms) or **all of them**.

A "payment system" as unstated in India, can include the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or such similar operations.

Operational Mechanism:

Under mobile or electronic wallet, the entity pre-load cash in the e-wallet and apply it to make payments or transfers. Loading of money is done either electronically using a computer / mobile by debiting from a credit card or bank account or physically by handover cash at a local merchant or at the ATM counters. There are charges for use of mobile / e-wallet, which comprise registration fees and cash loading charges towards payment companies / service providers. These charges are at times advanced than those for Internet banking. However, the major advantage with the e-wallet is that while shopping online, the customer stands to profit from the concessions/ offers from the payment companies in the form of cash-backs etc.

Benefits of e-wallets:

Use of debit cards requires access to designated point of sales and ATM counters. However, in container of e-wallets, money moves along with the holder and he can access it from a tool held in his hand – his mobile or computer, giving a lot of flexibility for the account holder. Supplementary e-wallets avoid the dangers connected with card thefts.

For those who live far away from ATM / bank branches, as in the case of rural areas, money is still accessible to them at the click of a button. In case of any obligation for material cash, they just need to go to the nearby banking correspondent or a local merchant who can double up like an ATM machine.

11.8 Micro Payment

A micro payment is an e-commerce transaction involving a very little sum of money in exchange for impressive made available online, such as an request download, a service or Web-based content. Micro payments are sometimes defined as anything less than 75 cents and can be as low as a fraction of a cent. A special type of system is required for such payments, which are too small to be feasible for processing through credit card companies.

Here's one scheme for micro payment: The user and seller each establish an account with a third-party service provider who monitors, collects and distributes micro payments. The seller encodes per-fee links inside a Web page. When the user initiates a transaction, payment goes through an Internet wallet account managed by the service provider. Micro payments accumulate until they are collected as single, larger payments. Such a system is helpful when a user wants to make one-time micro payments to multiple sellers. Seller-based accounts are more common for repeat business with an individual enterprise.

11.9 Peer to Peer Payment

It is an online arrangement that allows individual members to entire financial transactions with one another by using an auction approach process that lets members offer loans for a definite amount and at a specific rate.

Operation:

Buyers have the alternative to gaze for a quantity and rate of interest that meet their needs. All members are categorized by their threat level. Members can glance through for new people based on diverse demographic information. Since P2P banking does not exercise third party banking institution intermediaries the rates and conditions are often much more favorable for the members.

Unlike conservative banking where the spread between deposit rates and lending rates are enthusiastic to finance the bank's administrative and logistic expenses, both lenders and borrowers get to hoard such costs, while paying assured commission to the P2P portal provider and/or the credit rating agency. With the advent of peer-to-peer payments, splitting tabs and bills with associates, friends and family has never been more convenient.

Paying friends, associates and family by phone or computer was first popularized by PayPal and has since been offered by Google and others. The service is increasingly obtainable through banks and credit unions, too, and on social media networks like Flipkart, Amazon, home shop 18 and Snapdeal.

11.10 B2B and B2C Transactions

Customer Service takes multiplicity of forms based on the environment of the business and the objective market. Historically B2B and B2C categories of customer service followed self-governing paths in their growth. However there has been some junction and cross-pollination of thoughts, innovations, and best practices across these categories. Let’s catch a look at the fundamentals of both Business Models:

Business-to-business (B2B):

B2B describes commerce transactions between businesses, such as between a producer and a wholesaler, or between a wholesaler and a retailer.

Business-to-consumer (B2C):

B2C (sometimes also called Business-to-Customer) describe activities of businesses serving end consumers with products and/or services.

General Buying Cycle

1. Acknowledging the require
2. Awareness
3. Research
4. Consideration (the short list)
5. Evaluation
6. Purchase
7. Applications
8. The Experience
9. Reaction
10. Opportunity for advocacy

11.11 Advantages and Disadvantages

In the Age of High Technology cash strives to endure the competition with electronic money, because more and more people prefer to have virtual-wallets. It is clear, electronic payment systems have a range of pros in comparison to banking-services:

Advantages:-

1. **Time savings:**

   Money transfer between virtual accounts usually takes a few minutes, while a wire transfer or a postal one may take several days. Also, you will not waste your time waiting in lines at a bank or post-office.

2. **Expenses control:**

   Even if someone is eager to bring his disbursements under control, it is necessary to be patient enough to write down all the petty expenses, which often takes a large part of the total amount of disbursements. The virtual account contains the history of all transactions indicating the store and the amount you spent. This advantage of electronic payment system is pretty important in this case.

3. **Reduced risk of loss and theft:**

   You cannot forget your virtual wallet somewhere and it cannot be taken away by robbers.

4. **Low commissions:**

   Customer paid for Internet service provider or mobile account replenishment through the UPT (unattended payment terminal). As for the electronic payment system, a fee of this kind of operations consists of 1% of the total amount, and this is a considerable advantage.

5. **User-friendly:**

   Usually each service is designed to reach the widest possible audience, so it has the intuitively understandable user interface. In addition, there is always the opportunity to submit a question to a support team, which often works 24/7.

6. **Convenience:**

   All the transfers can be performed at anytime, anywhere. It's enough to have an access to the Internet.

Disadvantages:

1. Restrictions:

   Each payment system has its limits regarding the maximum amount in the account, the number of transactions per day and the quantity of output.

2. The risk of being hacked:

   If you pursue the security rules the risk is minimal, it can be compared to the threat of something similar to a robbery. The poorer situation when the system of giving out company has been broken, because it leads to the escape of personal data on cards and its owners. Even if the electronic payment system does not initiate plastic cards, it can be complicated in scandals regarding the Identity theft.

3. The problem of transferring money between different payment systems:

   Usually the popular of electronic payment systems do not cooperate with each other. In this case, you have to use the services of e-currency replace, and it can be time-consuming if you still do not have a trusted refurbish for this reason.

4. The lack of anonymity:

   The information about all the transactions, including the total amount, time and recipient are stored in the database folder of the payment system and it means the intelligence bureau has an access to this information.

5. The necessity of Internet access:

   If Internet connection fails, you cannot access to your online account.

11.12 Self Learning Exercise

Q.1 Which of the following describes e-commerce?

a) Doing business electronically

b) Doing business

c) Sale of goods

d) All of the above

Q.2 Which of the following is part of the four main types for e-commerce?

a) B2B

b) B2C

c) C2B

d) All of the above

Q.3 Which segment do eBay, Amazon.com belong?

a) B2Bs

b) B2Cs

c) C2Bs

d) C2Cs

Q.4 Which type of e-commerce focuses on consumers dealing with each other?

a) B2B

b) B2C

c) C2B

d) C2C

Q.5 Which segment is e-Bay an example?

a) B2B

b) C2B

c) C2C

d) None of the above

Q.6 Which type deals with auction?

a) B2B

b) B2C

c) C2B

d) C2C

Q.7 In which website Global Easy Buy is facilitated?

a) Ebay.com

b) Amazon.com

c) Yepme.com

d) None of these

Q.8 The best products to sell in B2C e-commerce are:

a) Small products

b) Digital products

c) Specialty products

d) Fresh products

Q.9 Which products are people most likely to be more uncomfortable buying on the Internet?

a) Books

b) Furniture

c) Movies

d) All of the above

Q.10 Which products are people most likely to be comfortable buying on the Internet?

a) Books

b) PCs

c) CDs

d) All of the above

Q.11 Digital products are best suited for B2C e-commerce because they:

a) Are commodity like products

b) Can be mass customized and personalized

c) Can be delivered at the time of purchase

d) All of the above

Q.12 The solution for all business needs is:

a) EDI

b) ERP

c) SCM

d) None of the above

Q.13 All of the following are techniques B2C e-commerce companies use to attract customers, except:

a) Registering with search engines

b) Viral marketing

c) Online ads

d) Virtual marketing

Q.14 Which is a function of E-commerce?

a) marketing

b) advertising

c) warehousing

d) all of the above

Q.15 Which is not a function of E-commerce?

a) marketing

b) advertising

c) warehousing

d) none of the above

11.13Summery

E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless financial transactions. Electronic payment has revolutionized the business processing by sinking paper work, transaction costs, labor cost. Some of the modes of electronic payments are following.

- Credit Card
- Debit Card

- Smart Card
- E-Money
- Electronic Fund Transfer (EFT)

Credit Card:

Payment using credit card is one of most ordinary mode of electronic payment. Credit card is tiny plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to understand credit card via card readers. Following are the important constraints in the credit card system.

- The card holder - Customer
- The merchant - seller of product who can accept credit card payments.
- The card issuer bank - card holder's bank
- The acquirer bank - the merchant's bank
- The card brand - for example visa or MasterCard.

Debit Card:

Debit card, like credit card is a tiny plastic card with a unique number mapped with the bank account number. It is requisite to have a bank account before getting a debit card from the bank. The major variation between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account directly and there should be enough balance in bank account for the transaction to get finished whereas in case of credit card there is no such compulsion. Debit cards free customer to take cash, cheques and even merchants accepts debit card more readily. Having limit on amount being in bank account also helps customer to keep a cheque on his/her spending.

Smart Card:

Smart card is once more parallel to credit card and debit card in exterior but it has a small microprocessor chip embedded in it. It has the capacity to stock up customer work related/personal information. Smart card is also used to accumulate money which is concentrated as per usage. Smart card can be accessed only using a PIN of customer. Smart cards are safe as they stores information in encrypted format and are less expensive/provide quicker processing.

E-Money:

E-Money transactions refer to condition where payment is done over the network and amount gets transferred from one financial body to another financial body without any participation of a middleman. E-money transactions are faster, convenient and save a lot of time. Online payments complete via credit card, debit card or smart card is examples of e-money transactions. In case of e-cash, in cooperation customer and merchant both have to sign up with the bank or company issuing e-cash.

Electronic Fund Transfer:

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer. Internet based EFT is getting popularity. In this case, customer uses website provided by the bank. Customer logins to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers amount to other account if it is in same bank otherwise transfer request is forwarded to ACH (Automated Clearing House) to transfer amount to other account and amount is deducted from customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank.

11.14Glossary

EDI: Electronic Data Interchange

EFT: Electronic Fund Transfer

UPT : unattended payment terminal

11.15Answers to Self Learning Exercise

Q.1 (a)	Q.2 (d)
Q.3 (b)	Q.4 (d)
Q.5 (d)	Q.6 (d)
Q.7 (a)	Q.8 (b)

Q.9 (b)   Q.10 (d)

Q.11 (d)   Q.12 (b)

Q.13(d)   Q.14 (d)

Q.15 (c)

11.16 Exercise

Q.1 What is e-commerce? Discuss B2B2C and C2B2C model giving proper examples.

Q.2 Define Electronic Data Interchange. What are the components of Electronic Data Interchange?

Q.3 Explain how E-cash is used for secure transaction. Explain the advantages of e-commerce.

Q.4 What role does various types of cards play in Business to Business model?

Q.5 Discuss e-governance. Explain the Business to Administration model.

Q.6 Discuss in brief virtual auction. Explain the differences between virtual auction and reverse auction.

Q.7 What is Firewall? State the function of Firewall in e-commerce.

Q.8 Write short notes: -

a) RSA algorithm.

b) Trade cycle and describe the different stages of a Trade cycle.

Q.9 a) Define digital cash or e-cash. Explain with example how an online banking system works.

b) Explain the working principle of EFT.

Q.10 a) Distinguish between Credit and Debit card.

b) Explain EAN coding system for EDI message.

References and Suggested Readings

1. Web Commerce Technology Handbook, Minoli et al, McGraw Hill
2. Internet Commerce: Digital Models for Business, Lawrence et al, Wiley
3. Designing Systems for Electronic Commerce, Treese et al, Addison-Wesley
4. https://en.wikipedia.org/wiki/Electronic_data_interchange

UNIT-12

Intranet and Extranet

Structure of the Unit

12.19 References for more detailed study

12.0 Objective

The objective of this unit is to understand Network and Network Architecture, Internet, Intranet, Designing Extranet etc.

12.1 Introduction

An Intranet is a private network accessible only to an organization's staff. Generally a wide range of information and services from the organization's internal IT systems are available that would not be available to the public from the Internet. A company-wide intranet can constitute an important focal point of internal communication and collaboration, and provide a single starting point to access internal and external resources. In its simplest form an intranet is established with the technologies for local area networks (LANs) and wide area networks (WANs).Intranets are used to share information. Secure intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols. An intranet is a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

12.2 History

Corporate intranets began gaining popularity during the 1990s. Intranets quickly grew more complex as the result the concept of intranet portal was born. Today, intranet portals provide value-added capabilities such as managing workflows, increasing collaboration between work groups, and allowing content creators to self-publish their information. One typical example of a web platform used to build and host an intranet is Microsoft Sharepoint (**SharePoint** is a web based application that integrates with Microsoft Office. Launched in 2001, SharePoint is primarily sold as a document management and storage system, but the product is highly configurable and usage varies substantially between organizations.), which is used by 46% of organizations. It provides a lot of features necessary for collaboration, integration and customization.

12.3 Overview

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

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

12.4 Orientation

12.4.1 Network and its Architecture: Today the world scenario is changing. Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.

Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of computer network is Internet, Intranet, and Extranet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

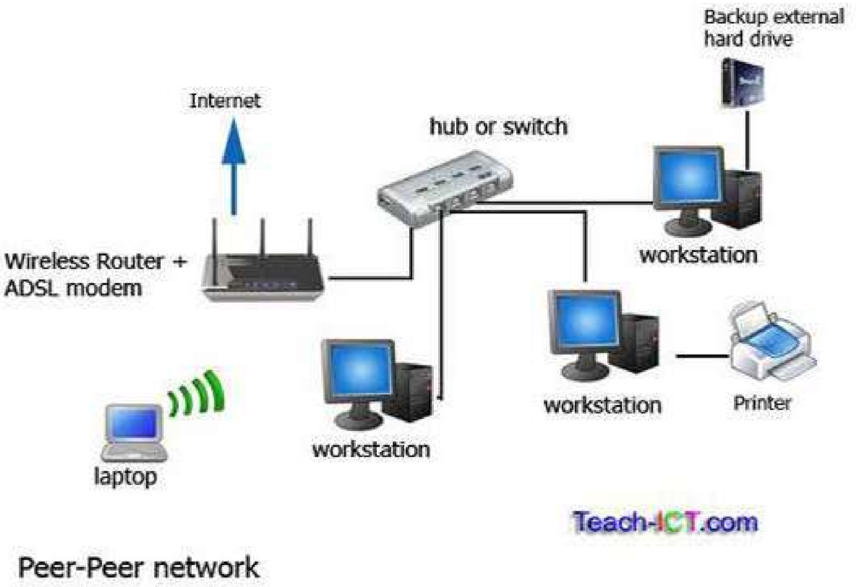


Fig. 12.1 Network Architecture with all peripherals

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology and organizational intent.

12.4.2 Brief about Protocols: In telecommunications, a communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. These are the rules or standard that defines the syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both. Communicating systems use well-defined formats (protocol) for exchanging various messages. Each message has an exact meaning intended to elicit a response from a range of possible responses pre-determined for that particular situation. The specified behavior is typically independent of how it is to be implemented. Communications protocols have to be agreed upon by the parties involved. To reach agreement, a protocol may be developed into a technical standard. A programming language describes the same for computations, so there is a close analogy between protocols and programming languages: protocols are to communications what programming languages are to computations. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together are known as a protocol suite; when implemented in software they are a protocol stack.

12.4.3 Firewalls and security: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network.

12.4.4 Authorized and Unauthorized Access: Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access it is considered unauthorized access. Unauthorized access could also

occur if a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access and possibly see an unauthorized access message. Some system administrators set up alerts to let them know when there is an unauthorized access attempt, so that they may investigate the reason. These alerts can help stop hackers from gaining access to a secure or confidential system.

Fig. 12.2 Unauthorized Accessing

12.4.5 Local Area Network and Wide Area Network: A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed. By contrast, a wide area network (WAN), not only covers a larger geographic distance, but also generally involves leased telecommunication circuits or Internet links. LANs can maintain connections with other LANs via leased lines, leased services, or across the Internet using virtual private network technologies. Depending on how the connections are established and secured, and the distance involved, such linked LANs may also be classified as a metropolitan area network (MAN) or a wide area network (WAN). Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks. Early LAN cabling had generally been based on various grades of coaxial cable. This led to the development of 10BASE-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. Many LANs are now based partly or wholly on wireless technologies. Smart phones, tablet computers and laptops typically have wireless networking support built-in. In a wireless local area network, users may move unrestricted in the coverage area. Wireless networks have become popular in residences and small businesses, because of their ease of installation. Guests are often offered Internet access via a hotspot service.

A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance. Wide area networks are often established with leased telecommunication circuits.

Business, education and government entities use wide area networks to relay data among staff, students, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet may be considered a WAN.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects the LAN on one side with a second router within the LAN on the other. Leased lines can be very expensive.

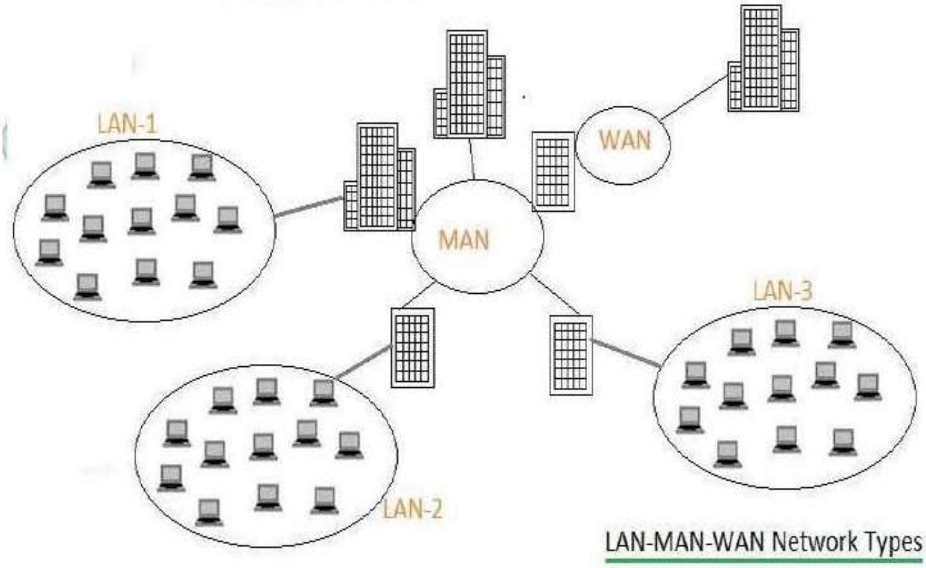


Fig 12.3 Consolidated diagram of LAN-MAN-WAN

12.5 Intranet

An intranet is a private network accessible only to an organization's staff. Generally a wide range of information and services from the organization's internal IT systems are available that would not be available to the public from the Internet.

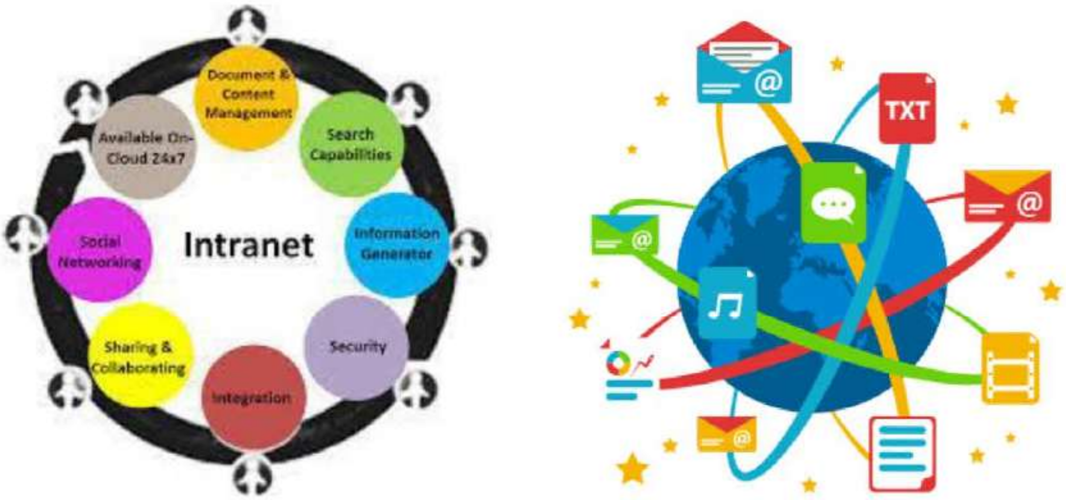


Fig.12.4 Intranet work facilities and application contents

A company-wide intranet can constitute an important focal point of internal communication and collaboration, and provide a single starting point to access internal and external resources. In its simplest form an intranet is established with the technologies for local area networks (LANs) and wide area networks (WANs).

12.6 Planning & Creation of Intranet

Intranet is designed with a strategic importance to the organization's success, determining the purpose and goals, identifying persons or departments responsible for implementation and management and devising functional plans, page layouts and designs regarding the input of new data and updating of existing data are to be centrally controlled or devolve. The appropriate staff would also ensure that implementation schedules and phase-out of existing systems were organized, while defining and implementing security of the intranet and ensuring it lies within legal boundaries and other constraints. In order to produce a high-value end product, systems planners should determine the level of interactivity (e.g. wikis, on-line forms) desired. Intranets are often static sites; they are a shared drive, serving up centrally stored documents alongside internal articles or communications (often one-way communication). By leveraging firms which specialize in 'social' intranets, organizations are beginning to think of how their intranets can become a 'communication hub' for their entire team.

12.7 Managing the Intranet

a) Split Available Time in an Effective Manner

b) Ensure that Notifications are Going Out

c) Determine the Needs of Community Members

d) Start Things Off with a Solid Plan

e) Reward Employees via Gamification

f) Manage Time While Keeping Company Objectives in Mind

g) Maintain a Strong Brand Identity on the Intranet

h) Ensure that High-level Support and Involvement Exists

i) Publish and Maintain Content

j) Don't Neglect the Importance of an Internal Newsletter

k) Provide Support

l) Keep Your Intranet Organized

m) Set Permissions

n) Make Sure Old Content Gets Archived

o) Look towards the Future

p) Pay Attention to Intranet Trends

q) Encourage Adoption

r) Measure Your Successes

s) Fix Technical Issues

t) Facilitate Collaboration

Activities of Intranet:

Tools & Resources: Area for employees to link to or download necessary applications to perform work functions. Information also provided to find internal and external resources.

Associate Services as follows:

Business Operations: To give users access to important business policies and manuals.

Company Calendar: It gives user access to important company event dates and times.

Access Point for Employees: Location for employees default main company webpage to obtain all information regarding the company.

Wiki: It can be used in the business environment for knowledge management.

Workflow Management: Establish work flows for common business tasks such as submitting expense reports, submitting corporate HR paperwork and document approval processes.

Bulletin Board: Manage corporate announcements.

Task Management: Create and update shared task lists throughout the corporation.

12.8 Intranet Portal

An intranet portal is the gateway that unifies access to enterprise information and applications on an intranet. It is a tool that helps a company manage its data, applications, and information more easily, and through personalized views. Some portal solutions today are able to integrate legacy applications, objects from other portals, & handle thousands of user requests. In a corporate enterprise environment, it is also known as an *enterprise portal*.

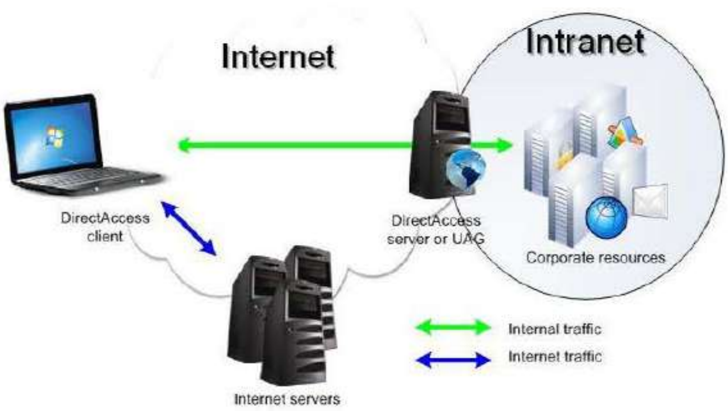


Fig. 12.5 Intranet portal planning with Internet

a) Intranet portal Features:

Integration: Intranet has ability to integrate with your current tools or the possibility of adding new tools. You have your outlook calendar and email integrated within intranet.

Security: Enable user or group based security to secure documents and sites throughout the intranet portal.

Customization: It uses Software that is flexible to allow for organization. Web Parts can be used to create custom modules which can make interaction easier with the site. Ability for users to customize tools and resources they use most often.

Collaboration: People are now able to add their work with each other. Example would be multiple people working on one document.

Communication Channels: Allows corporations to promote corporate culture and present information in a more interactive way than before.

Automation: Things like workflows and templates can automate specific document creation. Alerts can be created to help learn of changes and new additions to the intranet.

Applications: Links to applications for associates to perform duties.

User Friendly: Application must be easy to use and understand due to a wide range of technical abilities.

Remote Access: Intranet has Ability for users to access content away from the office.

Document Repository: Intranet has Ability to store and retrieve document information while maintaining regular backups to prevent data loss.

Blog: It is used as a method to provide more timely information to employees, customers, and business partners.

People Search: Search enterprise wide for employee information such as contact information, specialty areas, group membership, personal interest, etc.

Enterprise Search: It search enterprise content using enterprise search.

Targeted Content: Business portal administrators can target content by business group area, e.g., HR, Marketing, Legal, Corporate Executives, etc.

b) Benefits and Applications:

Workforce productivity: Intranets can help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database the organization wants to make available, anytime and — subject to security provisions — from anywhere within the company workstations, increasing the 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.

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.

Communication: Intranets can serve as powerful tools for communication within an organization, vertically strategic initiatives that have a global reach throughout the 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. Some examples of communication would be chat, email, and/or blogs. A great real-world example of where an intranet helped a company communicate is when Nestle had a number of food processing plants in Scandinavia. Their central support system had to deal with a number of queries every day. When Nestle decided to invest in an intranet, they quickly realized the savings. McGovern says the savings from the reduction in query calls was substantially greater than the investment in the intranet.

Web publishing: It allows cumbersome corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. Examples include: employee manuals, benefits documents, company policies, business standards, news feeds, and even training, can be accessed using common Internet standards (Acrobat files, Flash files, CGI applications). Because each business unit can update the online copy of a document, the most recent version is usually available to employees using the intranet.

Business operations and management: Intranets are also being used as a 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 physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating documents, and the environment as well as document maintenance overhead.

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

Cross-platform capability: Standards-compliant web browsers are available for Windows, Mac, and UNIX.

Built for one audience: Since Intranets are user-specific (requiring database/network authentication prior to access), you know exactly who you are interfacing with and can personalize your Intranet based on role (job title, department) or individual ("Congratulations Jane, on your 3rd year with our company!").

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

Immediate updates: When dealing with the public in any capacity, laws, specifications, and parameters can change. Intranets make it possible to provide your audience with "live" changes so they are kept up-to-date, which can limit a company's liability.

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

Intranet applications:

Intranet applications are same as that of Internet applications. Intranet applications are also accessed through a web browser. The only difference is that, Intranet applications reside on local server while Internet applications reside on remote server. Here, we've discussed some of these applications:-

1) **Document publication applications**: Document publication applications allow publishing documents such as manuals, software guide, employee profits etc without use of paper.
2) **Electronic resources applications:** It offers electronic resources such as software applications, templates and tools, to be shared across the network.
3) **Interactive Communication applications**: Like on internet, we have e-mail and chat like applications for Intranet, hence offering an interactive communication among employees.
4) **Support for Internet Applications**: Intranet offers an environment to deploy and test applications before placing them on Internet.

c) Advantages and Disadvantages:

Advantages: - Intranet portal helps employees make better and more informed decisions, which result from increased knowledge. It also helps reduce costs, saves time, increases collaboration, increases productivity and effectiveness. Intranet portal can help employees find information more easily and perform their jobs better, though few portal designs are optimal just out-of-the-box. In fact, especially in smaller companies, designers can realize some features found in off-the-shelf portal software through simpler (do-it-yourself) means. Most intranets have become completely unwieldy and present a highly fragmented and confusing user experience, with no consistency and little navigational support. Portals aim to correct this problem by presenting a single gateway to all corporate information and services. One benefit of creating this consistent look and feel is users need less time to learn how to use the environment. They also more easily recognize where they are in the portal and where they can go no small feat when navigating a large information space. By integrating services and presenting personalized snippets on the initial screen, intranet portals also reduce the need for users to browse far and wide to obtain needed information, thus making it easier for them to perform their jobs. Intranet portal is a Web-based tool that allows users to create a customized site that dynamically pulls in Internet activities and desired content into a single page. By providing a contextual framework for information, portals can bring S&T (Science and Technology) and organizational "knowledge" to the desktop.

1. **Time savings:**

   Money transfer between virtual accounts usually takes a few minutes, while a wire transfer or a postal one may take several days. Also, you will not waste your time waiting in lines at a bank or post-office.

2. **Expenses control:**

   Even if someone is eager to bring his disbursements under control, it is necessary to be patient enough to write down all the petty expenses, which often takes a large part of the total amount of disbursements. The virtual account contains the history of all transactions indicating the store and the amount you spent. This advantage of electronic payment system is pretty important in this case.

3. **Reduced risk of loss and theft**:

You cannot forget your virtual wallet somewhere and it cannot be taken away by robbers.

4. **Low commissions:**

   Customer paid for Internet service provider or mobile account replenishment through the UPT (unattended payment terminal). As for the electronic payment system, a fee of this kind of operations consists of 1% of the total amount.

5. **User-friendly:**

   Usually each service is designed to reach the widest possible audience, so it has the intuitively understandable user interface. In addition, there is always the opportunity to submit a question to a support team, which often works 24/7.

6. **Convenience:**

   All the transfers can be performed at anytime, anywhere. It's enough to have an access to the Internet.

Disadvantages: - Intranet Portals can be a large business cost. The maintenance and management can be time consuming and expensive. Not only is it a cost to keep the portal running but a cost when the system goes offline. Most intranets are established to put all an organization's resources into one place and having that offline can force operations to be put on hold. Security issues can become an ongoing problem. Unauthorized access is a concern and can result in users gaining access to sensitive information. Denial of access can cause issues for users needing access for their work. Having everything in one place is only good if it's organized. Information overload can make finding information very difficult lowering productivity.

1. **Restrictions:**

   Each payment system has its limits regarding the maximum amount in the account, the number of transactions per day and the quantity of output.

2. **The risk of being hacked:**

   If you pursue the security rules the risk is minimal, it can be compared to the threat of something similar to a robbery. The poorer situation when the system of giving out company has been broken, because it leads to the escape of personal data on cards and its owners. Even if the electronic payment system does not initiate plastic cards, it can be complicated in scandals regarding the Identity theft.

3. **The problem of transferring money between different payment systems:**

   Usually the popular of electronic payment systems do not cooperate with each other. In this case, you have to use the services of e-currency replace, and it can be time-consuming if you still do not have a trusted refurbish for this reason.

4. **The lack of anonymity:**

   The information about all the transactions, including the total amount, time and recipient are stored in the database folder of the payment system and it means specifically the intelligence bureau of any country may have an access to this information.

5. **The necessity of Internet access:**

   If Internet connection fails, you cannot access to your online account.

12.9 Designing an Extranet

An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet. An extranet is similar to a DMZ in that it provides access to needed services for authorized parties, without granting access to an organization's entire network. An extranet is a private network organization.

This means to say that an extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.

12.10 The cost of Setting up and Running of an Extranet

In terms of technology, an extranet can be little more than a regular Web site with password protection (that is, a person must have a password to enter). Another option is to build the extranet as a VPN. Companies can build their own extranets, but they usually tap an outside expert to do the work because it requires specialized technology.

Cost can be a deterrent to extranet construction. Global companies often spend up to $300,000 to create an extranet, and millions more to provide specialized functions such as advanced inventory data or sharing financial information with joint-venture partners. However, smaller firms can set up a basic extranet for a few thousand dollars if they already have a Web site and an intranet.

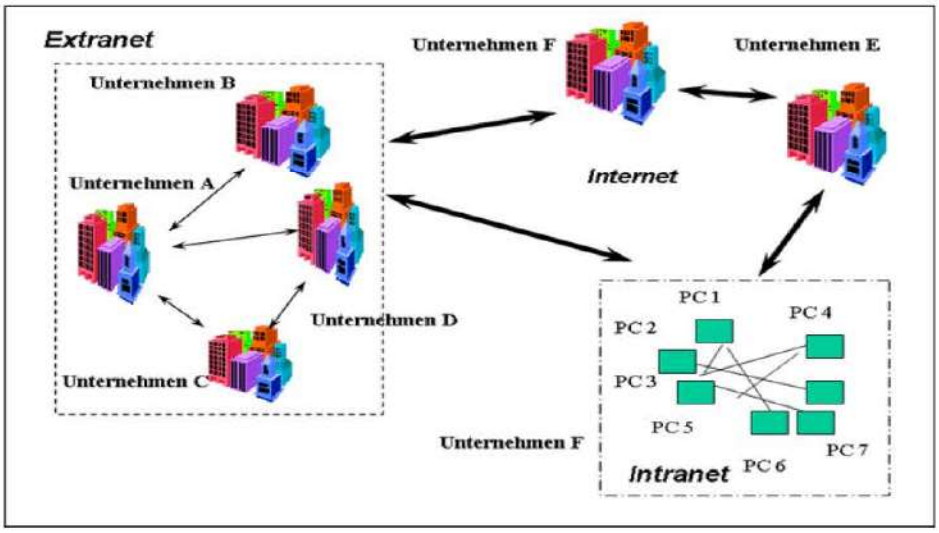


Fig. 12.6 Intranet-Extranet-Internet network architecture

12.11 Company use of an Extranet

The integral steps to developing an extranet are:

- **Discovery.** The process should begin with "discovery." It's very likely that a medium to large company already has components of an extranet in place - both IT and business units are allowing ad hoc access to company resources to important partners. If this is true, it's important to identify each of these pre-existing relationships and assess their needs today and in the foreseeable future. Only after that assessment is done can a positive, definitive extranet policy be established.

- **Architecture Definition.** An extranet is a customer service application disguised as a management and security problem. The perspective that technology decision makers must take is two-fold: How can I enable the richest access to services for our partners while simultaneously protecting the security and management interests of my internal data owners? An architecture must be defined that allows broad application access for partners — enough to keep them coming back for more — while allowing authorized access only.
- **Live Pilot**. It's important to conduct a realistic pilot using external partners, so pilot early with an outsider. Some organizations make the mistake of presuming that internal users will be able to raise all the important technology issues that an extranet raises: Authorization, firewall traversal, and support for wide scale heterogeneity.

Companies can use an extranet to:

- Exchange large volumes of data using Electronic Data Interchange (EDI)
- Share product catalogs exclusively with wholesalers or those "in the trade"
- Collaborate with other companies on joint development efforts
- Jointly develop and use training programs with other companies
- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks
- Share news of common interest exclusively with partner companies

12.12 Advantages and Disadvantages of Extranet

Advantages:

- Exchange large volumes of data using Electronic Data Interchange (EDI)
- Share product catalogs exclusively with trade partners
- Collaborate with other companies on joint development efforts

- Jointly develop and use training programs with other companies
- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks

Disadvantages:

- Extranets can be expensive to implement and maintain within an organization (e.g., hardware, software, employee training costs), if hosted internally rather than by an application service provider.
- Security of extranets can be a concern when hosting valuable or proprietary information.

12.13 Benefits of Implementing Extranet

There is a great deal of reasons why it might be beneficial for your business to implement an extranet.

- **An extranet can streamline repetitive business processes:** Let's say you order from a particular vendor on a regular basis, often using email or phone as a conduit. With a well-designed extranet, all of your ordering can take place via your secured private network in a virtual space. Any interactions with vendors occur in real time, and you can store invoices along with any other pertinent information in one place. This makes it easy to refer back to purchases you've made in the past. Keeping everything in the same virtual space not only cuts down on wasted time, but comes along with a wealth of organizational benefits.
- **It can increase customer satisfaction:** One of the key benefits of an extranet is that it can be accessed from any computer at any time of the day or night. 24/7 access means that your clients and customers can upload documents, ask questions, or approve designs/concepts whenever they have the time to do so, thus breaking down the barriers often caused by a more rigid work schedule.
- **Extranets are beneficial because they are highly secure when properly designed:** In some industries (medical, insurance, etc.), security is of the

utmost importance, and a breach could end in disaster. In many ways, email and other tools that are often used to transfer documents lack the type of security necessary to avoid a potential breach. When care is taken in designing an extranet, these concerns are no longer an issue.

12.14 INTRANET V/S EXTRANET

The difference between an intranet and an extranet is:

- An *intranet* is a network where employees can create content, communicate, collaborate, get stuff done, and develop the company culture. Whereas an *extranet* is like an intranet, but also provides controlled access to authorized customers, vendors, partners, or others outside the company.
- **Intranets and extranets** are two different things, and both can be beneficial to businesses in any industry. Once integrated into a business model, these portals can make day to day activities more efficient, more streamlined, better connected, and more productive.
- Understanding the differences between extranets and intranet software isn't as difficult as you might think, and it requires little more than a brief background on each. The better you can grasp these concepts, the more likely it is that you'll benefit from putting them to use.

12.15Summary

Intranet: An intranet is a private network accessible only to an organization's staff. Generally a wide range of information and services from the organization's internal IT systems are available that would not be available to the public from the Internet. A company-wide intranet can constitute an important focal point of internal communication and collaboration, and provide a single starting point to access internal and external resources.

Extranet: An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet. An extranet is similar to a DMZ in that it provides access to needed services for authorized parties, without granting access to an organization's entire network. An extranet is a private network organization. This means to say that an extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.

Managing the Intranet:

a) Split Available Time in an Effective Manner
b) Ensure that Notifications are Going Out
c) Determine the Needs of Community Members
d) Start Things Off with a Solid Plan
e) Reward Employees via Gamification
f) Manage Time While Keeping Company Objectives in Mind
g) Maintain a Strong Brand Identity on the Intranet
h) Ensure that High-level Support and Involvement Exists
i) Publish and Maintain Content
j) Don't Neglect the Importance of an Internal Newsletter
k) Provide Support
l) Keep Your Intranet Organized
m) Set Permissions
n) Make Sure Old Content Gets Archived
o) Look towards the Future
p) Pay Attention to Intranet Trends
q) Encourage Adoption
r) Measure Your Successes
s) Fix Technical Issues
t) Facilitate Collaboration

Company use of an EXTRANET:

Companies can use an extranet to:

- ➢ Exchange large volumes of data using Electronic Data Interchange (EDI)
- ➢ Share product catalogs exclusively with wholesalers or those "in the trade"

- Collaborate with other companies on joint development efforts
- Jointly develop and use training programs with other companies
- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks
- Share news of common interest exclusively with partner companies

12.16 Self Learning Exercise

Q.1 Which of the following is not a scripting language?

a) HTML

b) XML

c) Postscript

d) Javascript

Q.2 A digital signature is

a) scanned signature

b) signature in binary form

c) encrypting information

d) handwritten signature

Q.3 Mechanism to protect private networks from outside attack is

a) Firewall

b) Antivirus

c) Digital signature

d) Formatting

Q.4 A computer system that permits multiple users to run programs at same time

a) Real time system

b) Multi programming system

c) Time sharing system

d) Multi tasking system

Q.5 A computer communication technology that provides a way to interconnect multiple computers across short distance is

a) LAN

b) MAN

c) WAN

d) Wireless network

Q.6 Telnet is a service that runs

a) Television on net

b) Remote program

c) Cable TV network

d) Telenext

Q.7 A device that forwards data packet from one network to another is called a

a) Bridge

b) Switch

c) Hub

d) Gateway

Q.8 Which of the following is the fastest media of data transfer?

a) Co-axial Cable

b) Untwisted Wire

c) Telephone Lines

d) Fibre Optic

Q.9 Tool that is used to transfer data/files among computers on the Internet

a) FTP

b) Archie

c) TCP

d) Gopher

Q.10 HTML is a

a) Programming Language

b) Scripting Language

c) Web Browser

d) Network Protocol

Q.11 Secret-key encryption is also known as

a) Asymmetric encryption

b) Symmetric encryption

c) Secret-encryption

d) Private encryption

Q.12 The concept of electronic cash is to execute payment by

a) Credit Card

b) ATM Card

c) Using computers over network

d) Cheque

Q.13 SMTP is a

a) Networking Protocol

b) Protocol used for transferring message between end user & Mail Server

c) Protocol used for smart card message interchange

d) Encryption Standard

Q.14 Digital Signature is

a) Scanned Signature on Computer

b) Code number of the sender.

c) Public Key Encryption.

d) Software to recognize signature.

Q.15 Telnet is a

a) Network of Telephones

b) Television Network

c) Remote Login

d) Remote Login.

12.17Answers to Self Learning Exercise

Q.1 (c)

Q.2 (c)

Q.3 (a)

Q.4 (d)

Q.5 (a)

Q.6 (b)

Q.7 (b)

Q.8 (d)

Q.9 (c)

Q.10 (b)

Q.11(d)

Q.12 (c)

Q.13 (b)

Q.14(d)

Q.15 (c)

12.18 Exercise

Q. 1 What is Intranet? Discuss its planning with suitable example.

Q.2 Define creation of Intranet in the designing of any network?

Q.3 Explain how Extranet is useful for Business. Explain the advantages of it.

Q.4 What role does Intranet in any organization?

Q.5 Discuss differences of Intranet and Extranet.

Q.6 Discuss in brief of advantages and disadvantages of Intranet and Extranet.

Q.7 What is Firewall? State the function of Firewall in Intranet.

Q.8 Write short notes: -

a) Intranet portal.

b) Applications of Intranet.

Q.9 Define Activities of Intranet in a organization.

Q.10 Explain the benefits of Intranet.

Q.11 Which applications can be extended to the extranet?

References and Suggested Readings

1. http://www.va-interactive.com/inbusiness/editorial/biztech/ibt/extranet
2. https://www.glasscubes.com/five-reasons-why-your-business-needs-an-extranet/
3. Internetwork design issues by Cisco systems, 2009
4. Guide to Securing Intranet and Extranet Servers - VeriSign, 2000
5. Understanding Networking Technologies by Clayton Coulter - Atrium Technical Inc., 1997

Unit-13
Legal Issues Related to Cyber Laws in India

Structure of the Unit:

13.0 Objectives

After going through this unit students will be able to Understand

- the meaning of Cyber Space and E-Commerce;
- What are crimes and cyber crimes?
- Characteristics of Cyber Crimes;
- The need for cyber law and legal framework of cyber space;
- the jurisprudence of Indian cyber laws in E-Commerce and cyber space;

13.1 Introduction

Very few of us have a limited knowledge of crime occurring in "cyberspace", known as cybercrimes, which happens on computer and the Internet, however, cyberspace has a severe potential for remarkable impact on the lives of individuals and on our society. Therefore, a detailed introduction of cyberspace needs to be understood. There are many terms used to describe cyberspace. The descriptions are "computer crimes", "computer-related crimes" or "crimes by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime are added to the definition. Also, Internet brought other new terms, like "cybercrimes" and "net crimes". Other forms includes "digital crimes", "electronic crimes", "virtual crimes", "IT crimes", "high-tech crimes" and technology-enabled" crimes. However, on the one hand, each of them didn't cover the whole meaning of cyberspace and its crimes, because there is no incorporation of networks. On the other hand, terms such as "high-tech" or "electronic" crimes might be too broad to specify that the crime is the exact cybercrimes, since other fields also have "hi-tech" developments like nanotechnology and bioengineering. Currently, although no one term has become totally dominant in use, "cyberspace" is the term used most pervasively.

In general, cyberspace has three categories:

1. Target cyberspace: the crime in which a computer is the target of the offense.
2. Tool cyberspace: the crime in which a computer is used as a tool in committing the offense.
3. Computer incidental: the crime in which a computer plays a minor role in committing the offense.

13.2 E- Governance and E- commerce in India

In past few years, a large number of initiatives have been undertaken by various State Governments and various Central Ministries to usher in an era of e-Government. Sustained efforts have been made at multiple levels to improve the delivery of public services and simplify the process of accessing them.

Electronic governance or **e-governance** is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.

E-Governance in India has steadily evolved from computerization of Government Departments to initiatives that encapsulate the finer points of Governance, such as citizen centricity, service orientation and transparency. Lessons from previous e-Governance initiatives have played an important role in shaping the progressive e-Governance strategy of the country. Due cognizance has been taken of the notion that to speed up e-Governance implementation across the various arms of Government at National, State, and Local levels, a program approach needs to be adopted, guided by common vision and strategy. This approach has the potential of enabling huge savings in costs through sharing of core and support infrastructure, enabling interoperability through standards, and of presenting a seamless view of Government to citizens.

The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the internet. The ultimate objective is to bring public services closer home to citizens, as articulated in the Vision Statement of National e-Governance Plan (NeGP).

"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"

The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects and 8 components, on May 18, 2006. In the year 2011, 4 projects - Health, Education, PDS and Posts were introduced to make the list of 27 MMPs to 31Mission Mode Projects (MMPs). The Government has accorded approval to the vision, approach, strategy, key components, implementation methodology, and management structure for National e-Governance Plan (NeGP). However, the approval of National e-Governance Plan (NeGP) does not constitute financial approval(s) for all the Mission Mode Projects (MMPs) and components under it. The existing or ongoing projects in the MMP category, being implemented by various Central Ministries, States, and State Departments would be suitably augmented and enhanced to align with the objectives of National e-Governance Plan (NeGP).

In order to promote e-Governance in a holistic manner, various policy initiatives and projects have been undertaken to develop core and support infrastructure. The major core infrastructure components are State Data Centers (SDCs), State Wide Area Networks (S.W.A.N), Common Services Centers (CSCs) and middleware gateways i.e. National e-Governance Service Delivery Gateway (NSDG), State e-Governance Service Delivery Gateway (SSDG), and Mobile e-Governance Service Delivery Gateway (MSDG). The important support components include core policies and guidelines on Security, HR, Citizen Engagement, Social Media as well as Standards related to Metadata, Interoperability, Enterprise Architecture, Information Security etc.[1]

Details of various services of government agencies can be seen through the http://digitalindia.gov.in/service-directory.

E-Commerce:

E-commerce is a transaction of buying or selling online through electronic devices. E- commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern E-commerce typically uses the World Wide Web for at least one part of the transaction's life cycle although it may also use other technologies such as e-mail etc.

E-commerce may employ some or all of the following electronic transactions:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media

[1] http://meity.gov.in/content/national-e-governance-plan

- Business-to-business (B2B) electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in retail for launching new products and services
- Online financial exchanges for currency exchanges or trading purposes.[2]

Thus it can be defined as the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. The term e-tail is also sometimes used in reference to transactional processes for online shopping.

Disputes related with "Commercial Transactions" are concerned with Business to Business and Business to Consumer transactions are generally dealt by various commercial laws. i.e.

1. Indian Contract Act, 1872
2. Companies Act, 2013
3. Foreign Exchange Management Act, 1999 (FEMA)
4. Securities and Exchange Boaerd of India, 1992 (SEBI)
5. The Transfer of Property Act, 1882
6. Negotiable Instrument Act, 1881
7. The Registration Act, 1908
8. Competition Act, 2002
9. The consumer Protection Act, 1986 etc.

There are some other laws too but transactions related to E commerce are mainly dealt under Information Technology Act, 2000.

E- Commerce in India:

In India, cash on delivery is the most preferred payment method, accumulating 75% of the e-retail activities.[3] Demand for international consumer products is growing much faster than in-country supply from authorized distributors and e-

[2] https://en.wikipedia.org/wiki/E-commerce

[3] translatemedia.com. 2015-02-06. Retrieved 2015-03-24.

commerce offerings. India had an internet user base of about 354 million as of June 2015[4] and is expected to cross 500 million in 2016.[5] Despite being the second-largest user-base in world, only behind China (650 million, 48% of population), the penetration of e-commerce is low compared to markets like the United States (266 million, 84%), or France (54 M, 81%), but is growing at an unprecedented rate, adding around 6 million new entrants every month.[6] The number of mobile internet users in India has reached 371 million by June 2016, and is on track to cross 500 million users by next year.[7] In India, cash on delivery is the most preferred payment method, accumulating 75% of the e-retail activities[8].

In India, the largest e-commerce companies in India are Flipkart, Snapdeal, Amazon India, and Paytm etc.

E-Kranti:

Government of India accords highest priority to the Digital India program that is an umbrella program for transforming India into a digitally empowered society and knowledge economy. The pillars 4 and 5 of the Digital India program, namely **'e-Governance: Reforming Government through Technology' and 'E-Kranti - Electronic Delivery of Services'** respectively are directly linked to the E-Kranti: National E-Governance Plan (NeGP) 2.0. The implementation of E-Kranti is vital for Digital India and for the delivery of e-governance, easy governance and good governance in the country.

The Union Cabinet in its meeting held on 25.03.2015 has approved the Approach and Key Components of E-Kranti that include, inter alia, the vision, mission, key principles of E-Kranti, Approach and Methodology, Program Management Structure and Implementation Strategy including 44 Mission Mode Projects and Core ICT Infrastructure. The vision of E-Kranti is "Transforming e-Governance for Transforming Governance" and its mission is "To ensure a Government-wide transformation by delivering Government services electronically to the citizens

[4] timesofindia-economictimes. Retrieved 4 May 2016

[55] Business Standard. 5 May 2016. Retrieved 23 May 2016.

[6] https://en.wikipedia.org/wiki/E-commerce_in_India

[7] http://economictimes.indiatimes.com

[8] translatemedia.com. 2015-02-06. Retrieved 2015-03-24.

through integrated and interoperable systems via multiple modes, while ensuring efficiency, transparency and reliability of such services at affordable costs."

The details on the e-Kranti are as follow:

- Office Memorandum on e-Kranti
- Approach and Methodology for e-Kranti
- Principles of e-Kranti
- Program Management Structure of e-Kranti
- Implementation Strategy of e-Kranti
- Presentation on e-Kranti[9]

13.3 Types of Crimes

Crimes are defined by criminal law, which refers to a body of federal and state rules that prohibit behavior the government deems harmful to society. If one engages in such behavior, they may be guilty of a crime and prosecuted in criminal court.

In today's society, criminal behavior and criminal trials are highly publicized in the media and commonly the storyline in hit television shows and movies. As a result, people may consider themselves well-informed on the different types of crimes. However, the law can be quite complicated.

There are many different types of crimes but, generally, crimes can be divided into four major categories, personal crimes, property crimes, inchoate crimes, **and Statutory Crimes**:

- **Personal Crimes** – ***"Offenses against the Person*"**: These are crimes that result in physical or mental harm to another person. Personal crimes include: Assault, Battery, False Imprisonment, Kidnapping, Homicide, Rape, sexual assault etc.
- **Property Crimes** – ***"Offenses against Property":*** These are crimes that do not necessarily involve harm to another person. Instead, they involve an interference with another person's right to use or enjoy their property.

[9] http://meity.gov.in/content/e-kranti

Property crimes include: Theft, Robbery, Burglary, Arson, Embezzlement, Forgery, False pretenses, Receipt of stolen goods etc.

- **Inchoate Crimes** – ***"Inchoate"*** translates into "incomplete", meaning crimes that were begun, but not completed. This requires that a person take a substantial step to complete a crime, as opposed to just "intend" to commit a crime. Inchoate crimes include: Attempt – any crime that is attempted like "attempted robbery", Conspiracy etc.
- **Statutory Crimes** – A violation of a specific state or federal statute and can involve either property offenses or personal offense. Statutory crimes include: Alcohol-related crimes such as drunk driving (DUI), Selling alcohol to a minor.

Crimes are often classified according to the level of seriousness, such as:

- **Felony**
  - more serious crimes such as murder, kidnapping and robbery
  - Carries a year or more in state prison.
- **Misdemeanor**

  Less serious crimes are known as such as shoplifting or Driving under the Influence of some Intoxication.

  - Usually carries a fine and jail sentence of less than a year, if at all.

    State laws may further divide the categories of crimes into subcategories. For example, Offenses against the Person may be divided into the categories of "Violent Crimes" and "Non-Violent Crimes". Some states also place sexual crimes in their own category. These categories are also developed for the purpose of sentencing.

Finally, crimes can also be divided according to criminal intent. The major intent categories are ***General Intent Crimes and Specific Intent Crimes.*** These labels refer to the state of mind that a defendant must have in order to be found guilty of a crime. This is a difficult concept to master, but can be very important to your defense if you are charged with a crime.[10]

[10] http://www.legalmatch.com/law-library/article/what-are-the-different-types-of-crimes.html

Some other kinds of crimes are also known as:

Crimes against Morality:

Crimes against morality are also called victimless crimes because there is not complainant, or victim. Prostitution, illegal gambling, and illegal drug use are all examples of victimless crimes.

White-Collar Crime

White-collar crimes are crimes committed by people of high social status who commit their crimes in the context of their occupation. This includes embezzling (stealing money from one's employer), insider trading, tax evasion, and other violations of income tax laws.

White-collar crimes generally generate less concern in the public mind than other types of crime, however in terms of total dollars; white-collar crimes are even more consequential for society. For example, the Great Recession can be understood as in part the result of a variety of white-collar crimes committed within the home mortgage industry. Nonetheless, these crimes are generally the least investigated and least prosecuted because they are protected by a combination of privileges of race, class, and gender.

Organized Crime

Organized crime is committed by structured groups typically involving the distribution and sale of illegal goods and services. Many people think of the Mafia when they think of organized crime, but the term can refer to any group that exercises control over large illegal enterprises (such as the drug trade, illegal gambling, prostitution, weapons smuggling, or money laundering).[11]

13.4 Types of Cyber Crimes

Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes are the crimes committed with the help of electronic devices making person or property as target. Cyber crimes can be classified under different categories which are as follows:

[11] http://sociology.about.com/od/Deviance/a/Types-Of-Crimes.htm

We can categorize Cybercrimes in two ways

The Computer as a Target:-using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon:-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Other classifications for Cyber Crimes are:

1. **Cyber Crimes against Persons:**

There are certain offences which affect the personality of individuals can be defined as:

- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Virus and Worm attack:** A program that has capability to infect other computer or program.
- **Programs** and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.
- **Harassment via E-Mails:** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Face book, Twitter etc. increasing day by day.

1. E-mail Spoofing: E-mail spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. E-mail Spamming: E-mail "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3 Sending malicious codes through email: E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. E-mail Bombing: E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails, Defamatory emails.

6. Email frauds.

- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account *malafidely*. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Crimes against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects person's properties which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
-
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

Trojan Attack:-

- The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.

- The name "Trojan Horse" is popular.

- Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the *trojan*.

- TCP/IP protocol is the usual protocol type used for communications, but some functions of the *trojans* use the UDP protocol as well.

3. **Cybercrimes against Government:**

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. Cybercrimes against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Cyber crimes under the IT Act, 2000:

- Tampering with Computer source documents – Sec.65
- Hacking with Computer systems, Data alteration – Sec.66
- Publishing obscene information – Sec.67

- Un-authorized access to protected system Sec.70 Breach of Confidentiality and Privacy – Sec.72
  - Publishing false digital signature certificates – Sec.73

Rates of cyber crimes[12] have increased alarmingly. The following data sufficiently speaks itself about it:

The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2011 to 2015. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014. The cases registered under the IPC increased by more than 7 times during the period between 2011 and 2015. Similar trend is observed in the number of persons arrested. The government also acknowledges the increase in the number of such crimes and that the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses has resulted in such an increase. **Maharashtra & Uttar Pradesh on the top in cyber crimes.**

13.5 Characteristics of Cyber Crimes

Characteristics of Cyber Crime[13]:

- Commission of an illegal act using a computer, its systems, or applications
- Unlawful acts wherein the computer is either a tool or a target or both
- Crimes Perpetrated in Computer Environment
- Criminals are young and smart with technology knowledge
- Trans-National /Inter State criminals
- Jurisdiction Issues
- Strong Audit trail
- Mostly non violent crimes
- Veil of Anonymity
- Sometimes difficult to work out because:

[12] https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

[13] http://gurgaon.haryanapolice.gov.in/character_cyberc.htm

- **Physical contact between the child and the perpetrator does not need to occur for a child to become a victim or for a crime to be committed.** Innocent pictures or images of children can be digitally transformed into pornographic material and distributed across the Internet without the victims' knowledge.
- **The Internet provides a source for repeated, long-term victimization of a child that can last for years, often without the victim's knowledge.** Once a child's picture is displayed on the Internet, it can remain there forever. Images can stay on the Internet indefinitely without damage to the quality of the image.
- **These crimes transcend jurisdictional boundaries, often involving multiple victims from different communities, states, and countries.** The geographic location of a child is not a primary concern for perpetrators who target victims over the Internet. Often, perpetrators travel hundreds of miles to different states and countries to engage in sexual acts with children they met over the Internet. Many of these cases involve local, state, federal, and international law enforcement entities in multiple jurisdictions.
- **Many victims of Internet crimes do not disclose their victimization or even realize that they have been victims of a crime.** Whereas children who experience physical or sexual abuse may disclose the abuse to a friend, teacher, or parent, many victims of Internet crimes remain anonymous until pictures or images are discovered by law enforcement during an investigation. The presumed anonymity of Internet activities often provides a false sense of security and secrecy for both the perpetrator and the victim.[14]

13.6 Cyber Laws in India – Legal Framework

Necessity of law is felt when offences are committed. Use of technology in the form of computers and mobiles etc. is not old one, it is new age development. Before year 2000 there was no specific law to deal with above stated cyber crimes. At that time the cyber offences were punished under than prevailing law IPC (Indian Penal Code). Than cyber crimes involve criminal activities that were traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. They were punished under IPC with those nomenclatures. Lately in the year 2000 the Information Technology Act,

[14] https://ojp.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01_5.html

2000 was passed to deal with such offences. As the technological development in this field is very fast and changing this Act of 2000 is also found insufficient in dealing with cyber crimes in India. The Act has been amended in 2008.

13.7 Information Technology (IT) Laws in India

The Information Technology Act, 2000 is the prime Cyber Law of India which gives protection to all e-enable activities and provides punishment for all illegal activities as defined and described under this Act. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997. Cyber laws are meant to set the definite pattern, some rules and guidelines that defined certain activities going on through internet legal and certain illegal activities and hence punishable. The IT Act, 2000 the Cyber Law of India, gives the legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

One cannot blame or regard government as complete failure in shielding numerous e-commerce activities on the firm basis of which this industry has got to its skies, but then the law cannot be regarded as free from ambiguities.

The salient features of the Information Technology Act, 2000:

They may briefly be understood as follows[15]:—

1. The Act provides legal recognition to e-commerce, which facilitates commercial e-transactions.

2. It recognizes records kept in electronic form like any other documentary record. In this way, at brings electronic transactions at par with paper transactions in documentary form.

3. The Act also provides legal recognition to digital signatures which need to be duly authenticated by the certifying authorities.

4. Cyber Law Appellate tribunal has been set up to hear appeal against adjudicating authorities.

[15] http://www.shareyouressays.com/121630/salient-features-of-the-information-technology-act-2000

5. The provisions of the I.T. Act have no application to negotiable instruments, power of attorney, trust, will and any contract for sale or conveyance of immovable property.

6. The Act applies to any cyber offence or contravention committed outside India by a person irrespective of his/her nationality.

7. As provided under Section 90 of the Act, the State Government may, by notification in 'Official Gazette' make rules to carry out the provisions of the Act.

8. Consequent to the passing of this Act, the SEBI had announced that trading of securities on the internet will be valid in India, but initially there was no specific provision for protection of confidentiality and net trading. This lacuna has been removed by the IT (Amendment) Act, 2008.

Objectives of IT Act, 2000

- It is objective of I.T. Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
- To give legal recognition to digital signature for accepting any agreement via computer.
- To provide facility of filling document online relating to school admission or registration in employment exchange.
- According to I.T. Act 2000, any company can store their data in electronic storage.
- To stop computer crime and protect privacy of internet users.
- To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
- To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

The contents of the Act are:

The object of The Information Technology Act, 2000 as defined therein is as under:-

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Towards that end, the said Act thereafter stipulates numerous provisions. The said Act aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. Act further states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act purports to facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles coming in the way of electronic commerce resulting from the glorious uncertainties relating to writing and signature requirements over the Internet. The Act also aims to fulfill its objects of promoting and developing the legal and business infrastructure necessary to implement electronic commerce.

Chapter-II of the said Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person by the use of a public key of the subscriber can verify the electronic record.

CHAPTER III of the Act details about Electronic Governance and provides *interalia* amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

The said chapter also details about the legal recognition of Digital Signatures. The various provisions further elaborate on the use of Electronic Records and Digital Signatures in Government Agencies. The Act further talks of publications of rules and regulations in the Electronic Gazette.

Chapter IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Bill.

Chapter IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer system etc. have been fixed as damages by way of compensation not exceeding Rs. 100,00,000/- to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

There is a provision in Chapter X which envisage the Cyber Regulations Appellate Tribunal shall be an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred. The said Tribunal shall not be bound by the principles of the Code of Civil Procedure but shall follow the principles of natural justice and shall have the same powers as those are vested in a Civil Court. Against an order or decision of the Cyber Appellate Tribunal, an appeal shall lie to the High Court.

Chapter XI of the said Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information which is obscene in electronic form, breach of confidentiality and privacy, misrepresentation, publishing Digital Signature Certificate false in certain particulars and publication for fraudulent purposes.

Hacking has been properly defined in Section 66 as, "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking." Further for the first time, punishment for hacking as a cyber crime prescribed in the form of imprisonment up to 3 years or with fine which may extend to Rs. 2,00,000/- or with both. This is a welcome measure as hacking has assumed tremendous importance in the present day scenario. On previous occasions, the web sites of the Government have been hacked into but no legal provision within the existing legislation could be invoked to cover "hacking" as a cyber crime. It shall now be possible to try and punish hackers under section 66 of the IT Act, 2000.

{**Amendments:** A major amendment was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.}

The said Act also provides for the constitution of the Cyber Regulations Advisory Committee which shall advice the government as regards any rules or for any other purpose connected with the said act. The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The said Act also has four Schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

The said IT Bill was tabled in Parliament in December, 1999 and was referred to the Standing Committee on Science and Technology, Environment and Forests for examination and report. The Standing Committee examined the said IT Bill 1999 and proposed some stringent measures to further strengthen the legal infrastructure of the IT Bill 1999. The most positive aspect of the said report was that it recommended the insertion of the definition and punishment for "hacking".

Looking from an overall perspective, the Information Technology Act, 2000 is a laudable effort by the Government to create the necessary legal infrastructure for promotion and growth of electronic commerce. As on date, the judiciary in India is reluctant to accept electronic records and communications as evidence. Even email has not been defined in the prevailing statutes of India and is not an accepted legal form of communication as evidence in a court of law as of today. The said IT Act, 2000 indeed is a step forward in that direction also.

From the perspective of the corporate sector, the IT Act 2000 and its provisions contain the following positive aspects:-

(A) The implications of these provisions for the corporate sector would be that email will now be a valid and legal form of communication in our country, which can be duly produced and approved in a court of law. The corporate today thrive on email, not only as the form of communication with entities outsides the company but also email is used as an indispensable tool for intra company communication. Till now it has been seen that the corporate in their intra company communications on email have not been very careful in using the language in such emails. Corporate will have to understand that they shall need to be more careful while writing emails, whether outside the company or within as the same with whatever language could be proved in the court of law, sometimes much to the detriment of the company. Even intra company notes and memos, till now used only for official purposes, shall also be coming within the ambit of the IT Act and will be admissible as evidence in a court of law. A possible consequence of the same for a typical wired company would be that any employee, unhappy with a particular email communication, whether in personal or received in a official or personal capacity, may make the said email as the foundation for launching a litigation in a court of law. Further, when a company executive sends an email to another executive in the company with some defamatory or other related material and copies the same to others, there are possibilities that he may land in litigation in a court of law.

(B) Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Till now, the growth of Electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

(C) Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction in the Act.

(D) The Act also throws open the doors for the entry of corporate in the business of being of being Certifying Authorities for issuing Digital Signatures Certificates. The Act does not make any distinction between any legal entities for being appointed as a Certifying Authority so long as the norms stipulated by the government have been followed.

(E) The Act also enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in the electronic form by means of such electronic form as may be prescribed by the appropriate Government. India is rapidly moving ahead in the field of electronic governance and it will not be long before governments start taking applications or issuing license, permit, sanction or approvals, by whatever name called, online. This provision shall be a great leveler as this will enable all kinds of companies to do a lot of their interaction with different government departments online, thereby saving costs, time and wastage of precious manpower.

(F) Corporate are mandated by different laws of the country to keep and retain valuable and corporate information. The IT Act enables companies legally to retain the said information in the electronic form, if :-

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

(G) The I. T. Act also addresses the important issues of Security which are so critical to the success of electronic transactions. The Act has also given a legal definition to the concept of secure digital signatures which would be required to have been passed through a system of a security procedure, as stipulated by the government at a later date. In the times to come, secure digital signatures shall play a big role in the New Economy particularly from the perspective of the corporate sector as it will enable a more secure transaction online.

In today's scenario, information is supreme. Information is stored on their respective computer systems by the companies apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages not exceeding Rs.100,00,000. This penalty of damages apply to any person who, without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network.

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

(H) Corporate in India can now take a sigh of relief as the IT Act has defined various cyber crimes and has declared them penal offences punishable with imprisonment and fine. These include hacking and damage to computer source code and often corporate face hacking into their systems and information. Till date, the corporate were in a helpless condition as there was no legal redress to such issue. But the IT Act changes the scene altogether.

However, despite the overwhelming positive features of the IT Act, 2000 for the corporate sector, there are a couple of issues that concern the corporate in the said Act:-

(1)The said step has come a bit late. With the phenomenon growth of Internet which doubles approximately every 100 days, the said Act should have been passed long time back.

(2)It may be pertinent to mention that the said Act purports to be applicable to not only the whole of India but also to any offence or contravention there under committed outside of India by any person. This provision in section 1(2) is not clearly and happily drafted. It is not clear as to how and in what particular manner; the said Act shall apply to any offence or contravention there under committed outside of India by any person. The enforcement aspect of the IT Act is an area of grave concern. Numerous difficulties are likely to arise in the enforcement of the said Act as the medium of Internet has shrunk the size of the world and slowly, national boundaries shall cease to have much meaning in Cyberspace.

(3)It is also strange that section 1(4) of the said Act excludes numerous things from the applicability of the IT Act. The Act does not apply to (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881; (b) a power of attorney as defined in section 1 A of the Powers-of-Attorney Act, 1882; (c) a trust as defined in section 3 of the Indian Trusts Act, 1882; (d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called; (e) any contract for the sale or conveyance of immovable property or any interest in such property. The said IT Act already excludes numerous important things. The Act talks about promoting electronic commerce and it begins by excluding immovable property from the ambit of electronic commerce- a reasoning which defies logic.

(4)The IT Act, 2000 does not touch at all the issues relating to Domain Names. Even Domain Names have not been defined and the rights and liabilities of Domain Name owners do not find any mention in the said law. It may be submitted that Electronic Commerce is based on the system of Domain Names and excluding such important issues from the ambit of India's First Cyber law does not appeal to logic.

(5)The IT Act, 2000 does not also deal at all with the Intellectual Property Rights of Domain Name owners. Contentious yet very important issues concerning Copyright, Trademark and Patent have been left untouched in the said law thereby leaving many loopholes in the said law.

(6)The IT Act talks about the use of electronic records and digital signatures in government agencies. Yet, strangely it further says in section 9, that this does not confer any right upon any person to insist that the document in questions should be accepted in electronic form. The control of the Government is apparent, as the Controller of Certifying Authorities has to discharge his functions subject to the general control and direction of Central Government. The Internet and the phenomenon of electronic commerce require that minimum hurdles and obstacles need to be put in their way. The Act seeks to bureaucratize the entire process of controlling electronic commerce. This is likely to result into consequences of delays and other related problems.

(7)As Cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defines in the IT Act are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act make it appear as if the offences detailed in the said IT Act are the only Cyber offences possible and existing. For example, cyber offences like cyber theft, cyber stalking, cyber harassment and cyber defamation are not covered under the Act.

(8)The IT Act talks of Adjudicating Officers who shall adjudicate whether any person has committed a contravention of any provisions of this Act of any rules, regulations, directions or order made there under. How these Adjudicating Officers will adjudicate the contravention of the Act has not been made clear or well defined. Further, it has also not been specified as to how the said Adjudicating Officers shall determine whether any contravention of the Act or any offence has been committed by any person outside India. Further, what authority would these

Adjudicating Officers have viz-a-viz persons outside India who have committed any cyber offences have not been defined. No definitive procedure for adjudication by Adjudicating Officers has been exhaustively spelt out by the IT Act. Further the territorial jurisdiction of the said Adjudicating Officers and also the Cyber Regulations Appellate Tribunal has not been defined.

(9)Section 55 of the IT Act states that no order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no Act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal. The said provision is *violative* of the Fundamental Rights of the citizens as are enshrined in Chapter III of the Constitution of India and the said provision is not expedient and is likely to be struck down by the courts. The Central Government cannot claim immunity in appointments to Cyber Appellate Tribunal, as the same is contrary to the spirit of the Constitution of India. Further, it may be submitted that if there is a defect in the constitution of a Cyber Appellate Tribunal, that goes to the root of the matter and renders all proceedings and acts of the said Cyber Appellate Tribunal null & *void abinitio.*

(10)Further the said IT Act talks of any agency of the government intercepting any information transmitted through any computer resource if the same is necessary in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence. This is one provision which is likely to be misused by future governments to suit their political motives as also for the purpose of victimization. No standards or provisions have been laid down by the IT Act, which define any conditions detailed above. The supporters of the cause of individual privacy and freedom see these provisions as a gross violation of individual freedom and that aforesaid conditions are unreasonable restrictions, which are not permissible in the context of the rapid growth of Internet.

(11)Further, the said IT Act is likely to cause a conflict of jurisdiction.

(12)Another major gray area is that the draconian powers given to a police officer not below rank of the Deputy Superintendent of Police under Section 80 of the Act have been left untouched. Nowhere in the world do be find a parallel such a wide an unrestricted power to given to any officer for the purpose of investigating and preventing the commission of a cyber crime. After all, the power given by the IT Act to the said DSP includes the power to " enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act." The said power has been given without any restrictions of any kind whatsoever. It is very much possible that the same is likely to be misused and abused in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under Section 80 and companies will not be able to escape potential harassment from the hands of the DSP . This area of the IT Act can be one of the greatest concerns for the government, the industry and the people at large.

(13)The biggest concern about the new Indian Cyber law relates to its implementation. The said Act does not lay down parameters for its implementation. Also when Internet penetration in India is extremely low and government and police officials, in general are not at all, computer savvy, the new Indian Cyber law raises more questions than it answers them. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the gray areas mentioned above.[16]

All said and done, The Information Technology Act, 2000 is a great achievement and a remarkable step ahead in the right direction. The IT Act is a first step taken by the Government of India towards promoting the growth of electronic commerce so that Electronic Commerce in India can leap frog to success. Despite all its failings, it is a first historical step. The other steps have to follow.

MMS porn case in which the CEO of bazee.com (an Ebay Company) was arrested for allegedly selling the MMS clips involving school children on its website is the most apt example in this reference. Other cases where the law becomes hazy in its stand includes the case where the newspaper Mid-Daily published the pictures of the Indian actor kissing her boyfriend at the Bombay nightspot and the arrest of Krishan Kumar for illegally using the internet account of Col. (Retd.) J.S. Bajwa.

[16] http://www.mondaq.com/india/x/13430/IT+internet/Cyberlaw+In+India+The+Information+Technology+Act+2000+Some+Perspectives

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Let's have an overview of the law where it takes a firm stand and has got successful in the reason for which it was framed. The important features of the Act are:

1. The E-commerce industry carries out its business via transactions and communications done through electronic records. It thus becomes essential that such transactions be made legal. Keeping this point in the consideration, the IT Act 2000 empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also puts forward the proposal for setting up the legal framework essential for the authentication and origin of electronic records / communications through digital signature.

2. The Act legalizes the e-mail and gives it the status of being valid form of carrying out communication in India. This implies that e-mails can be duly produced and approved in a court of law, thus can be a regarded as substantial document to carry out legal proceedings.

3. The act also talks about digital signatures and digital records. These have been also awarded the status of being legal and valid means that can form strong basis for launching litigation in a court of law. It invites the corporate companies in the business of being Certifying Authorities for issuing secure Digital Signatures Certificates.

4. The Act now allows Government to issue notification on the web thus heralding e-governance.

5. It eases the task of companies of the filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government. This will help in saving costs, time and manpower for the corporate.

6. The act also provides statutory remedy to the corporate in case the crime against the accused for breaking into their computer systems or network and damaging and copying the data is proven. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore ($200,000).

7. Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.

8. The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.

The IT Law 2000, though appears to be self sufficient, it takes mixed stand when it comes to many practical situations. It loses its certainty at many places like:

1. The law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.
2. The law even stays silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.
3. The act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.
4. Internet is a borderless medium; it spreads to every corner of the world where life is possible and hence is the cyber criminal. Then how come is it possible to feel relaxed and secured once this law is enforced in the nation??

The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time?

The IT Act is silent on filming anyone's personal actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention.

For example, many Delhi based newspapers advertise the massage parlors; and in few cases even show the 'therapeutic masseurs' hidden behind the mask, who actually are prostitutes. Delhi Police has been successful in busting out a few such rackets but then it is not sure of the action it can take…should it arrest the owners and editors of newspapers or wait for some new clauses in the Act to be added up?? Even the much hyped case of the arrest of Bajaj, the CEO of Bazee.com, was a consequence of this particular ambiguity of the law. One cannot expect an ISP to monitor what information their subscribers are sending out, all 24 hours a day.

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space. India is the 12th nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan.

But can the cyber laws of the country be regarded as sufficient and secure enough to provide a strong platform to the country's e-commerce industry for which they were meant?? India has failed to keep in pace with the world in this respect, and the consequence is not far enough from our sight; most of the big customers of India's outsourcing company have started to re-think of carrying out their business in India. Bajaj's case has given the strongest blow in this respect and have broken India's share in outsourcing market as a leader.

If India doesn't want to lose its position and wishes to stay as the world's leader forever in outsourcing market, it needs to take fast but intelligent steps to cover the glaring loopholes of the Act, or else the day is not far when the scenario of India ruling the world's outsourcing market will stay alive in the dreams only as it will be overtaken by its competitors.[17]

Offences and the corresponding penalties in the I. T. Act:

Section	**Offence**	**Description**	**Penalty**
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer	Imprisonment up to three years, or/and with fine up to ₹ 200,000

[17] http://cyberlawsindia.net/2sides.html

		source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹ 500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹ 100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹ 100,000
66D	Cheating using computer	If a person cheats someone using a computer resource or	Imprisonment up to three years,

	resource	communication.	or/and with fine up to ₹ 100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹ 200,000
66F	Acts of cyber terrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹ 1,000,000
67A	Publishing images	If a person publishes or transmits images containing a	Imprisonment up to seven years,

	containing sexual acts	sexual explicit act or conduct.	or/and with fine up to ₹ 1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹ 1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹ 1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or	Imprisonment up to three years, or/and with fine up to ₹ 200,000

		any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.	
69	Failure/refusal to decrypt data.	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.

70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹ 100,000

13.7 Purpose of Cyber Laws:

Objectives of Cyber law or I.T. legislation in India: The Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself are: ***"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal***

Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Act essentially deals with the following issues:

a) Legal Recognition of Electronic Documents;

b) Legal Recognition of Digital Signatures;

c) Offenses and Contraventions;

d) ***Justice Dispensation Systems for cyber crimes.***

13.8 Amendments in Information Technology Act

Amendment Act 2008: Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA. Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the IT Amendment Act are as follows:

- Focusing on data privacy
- Focusing on Information Security

- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

13.9 Ethics and Cyber Laws

ETHICS IN GENERAL

A guideline is needed to stop the current technology products from being exploited for example replicating original CDs and selling them as pirated software, this unethical behavior can be controlled by the code of conducts.

Unethical refers to any code of conducts that are not conforming to approved standards of social or professional or business behavior. Computer or cyber ethics is a system of moral standards or values used as a guideline for computer or electronic device users.

THE TEN COMMANDMENTS OF COMPUTER ETHICS

The United States Institute of Computer Ethics has come out with the Ten Commandments of Computer Ethics. These principles consider the effective code of conducts for the proper use of information technology. The Ten commandments of computer ethics are :

1. You shall not use a computer to harm other people.
2. You shall not interfere with other people's computer work.
3. You shall not snoop around in other people's computer files.
4. You shall not use a computer to steal.
5. You shall not use a computer to bear false witness.
6. You shall not copy or use proprietary software for which you have not paid.
7. You shall not use other people's computer resources without authorization or proper compensation.

8. You shall not appropriate other people's intellectual output.
9. You shall think about the social consequences of the program you are writing or the system you are designing.
10. You shall always use a computer in ways that ensure consideration and respect for your fellow humans.

UNETHICAL COMPUTER CODE OF CONDUCTS

With the advancement of ICT, it is easy for anyone to retrieve your information from the Internet. You may not realize that when you fill a form on the Internet, your information may be exposed and stolen.

Examples of unethical computer code of conducts include:

- modifying certain information on the Internet, affecting the accuracy of the information
- selling information to other parties without the owner's permission
- using information without authorization
- involvement in stealing software
- invasion of privacy

ETHICAL COMPUTER CODE OF CONDUCTS

Examples of ethical computer code of conducts include:

- sending warning about viruses to other computer users
- asking permission before sending any business advertisements to others
- using information with authorization[18]

The Center for Cyber Safety and Education an organization committed to certification of computer security professional has further defined its own code of ethics generally as:

1. Act honestly, justly, responsibly, and legally, and protecting the commonwealth.
2. Work diligently and provide competent services and advance the security profession.
3. Encourage the growth of research – teach, mentor, and value the certification.

[18] http://ictsmksh.blogspot.in/2010/02/computer-ethics.html

4. Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.

5. Observe and abide by all contracts, expressed or implied, and give prudent advice.

6. Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are qualified to perform.

7. Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

13.10 Summary

Cyber Space or Cyber World is the well-known words to everyone now a day. It is simply related to functioning of modern electronic devices. Using these modern electronic devices is fun and easy. In using these modern electronic devices there are lots of danger to the person himself and the person on the other end. One has to remain very cautious while using them. Knowingly or unknowingly one may commit cyber-crime or may become victim of cybercrime. There is Information Technology Act, 2000 is the law along with other laws to deal with such types of cybercrimes. There are some cyber ethics to minimize the cyber-crimes. One should try to follow to them to the possible extent.

E-Commerce: E-commerce is a transaction of buying or selling online through electronic devices.

Electronic governance or **e-governance** is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.

Virus and Worm attack: A program that has capability to infect other computer or program.

Cyber-Stalking: It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

- **Harassment via E-Mails:** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Face book, Twitter etc. increasing day by day.

1. E-mail Spoofing: E-mail spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. E-mail Spamming: E-mail "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3 Sending malicious codes through email: E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. E-mail Bombing: E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

Trojan Attack:-

- The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.
  - The name "Trojan Horse" is popular.
- Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the *trojan*.
- TCP/IP protocol is the usual protocol type used for communications, but some functions of the *trojans* use the UDP protocol as well.

13.11 Self Assessment tests

Exercise: A

Q.1. Discuss the characteristics and nature of E-Governance in India.

Q.2. Explain of Crimes and its various types.

Q.3. Discuss the characteristics of Cyber Crimes in India.

Q.4. Explain the status of Cyber laws in India.

Q.5. Suggest amendments in Information Technology laws in India.

Exercise:B

1. Trojan Horse is a…………

a) Computer b) E-mail

c) A computer Law d) A destructive Computer Program

2. What is E-Commerce:

a) E-commerce is a transaction of buying or selling online through electronic devices.

b) A computer program to commercial activities.

c) An e-mail to corrupt the computer.

d) A virus destroying computer.

3. The Information Technology Act was passed in year………..

a) 2000 b) 1999

c) 2002 d) 2003

4. Major Provisions of penalty in the Information Technology Act are in:

a) Section: Section: 35 to 41 b) Section: 45 to 51

c) Section: 55 to 61 d) Section:65 to 71

5. E-mail "bombing" is characterized by……..

a) E-mail originated from one source while it was actually sent from another source.

b) E-mail sending email to thousands and thousands of users.

c) E-mails are used to send viruses.

d) E-mails repeatedly sending an identical email message to a particular address.

Answers to Exercise:B

1. d 2. a 3. a 4. d 5. d

13.12 Suggested Readings

1. Prevention of Cyber Crimes and Fraud Management Paperback – 2017, by Indian Institute of Banking and Finance (Author), Vikas Book house, Pune.

2. Cyber Law-Law of Information Technology and Internet Paperback– Sep 2014, UBSPD, Delhi

3. Cyber Law- Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes Hardcover – 2012, by Aparna Viswanathan (Author), Jain Book agency, Delhi

4. Textbook on Cyber Law Paperback – 2016, by Pavan Duggal (Author), UBSPD

5. Cyberlaws, E-Commerce & M-Commerce, Author: Tabrez Ahmad, jain Book Agency, Delhi

6. Cyber Law Simplified (Information Technology Law), Author: Vivek Sood (Advocate), Jain Book Agency, Delhi