5-15-2000

# Multilingual interactive integrated multimedia based e-commerce

Amol S. Chobe
*Florida International University*

**DOI:** 10.25148/etd.FI14060813

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

# MULTILINGUAL INTERACTIVE INTEGRATED MULTIMEDIA BASED E-COMMERCE

A thesis submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE

in

COMPUTER ENGINEERING

by

Amol S. Chobe

2000

To: Dean Gordon R. Hopkins
College of Engineering

This thesis, written by Amol S. Chobe, and entitled Multilingual Interactive Integrated Multimedia based E-Commerce, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this thesis and recommend that it be approved.

Tadeusz M. Babij

Maria Martinez

Subbarao V. Wunnava, Major Professor

Date of Defense: May 15, 2000

The thesis of Amol S. Chobe is approved.

Dean Gordon R. Hopkins
College of Engineering

Dean Richard L. Campbell
Division of Graduate Studies

Florida International University, 2000

# DEDICATION

I dedicate this thesis to my family. Without their patience, understanding, support and love, the completion of this work would not have been possible.

# ACKNOWLEDGMENTS

I would like to thank my committee members: Dr. Subbarao V. Wunnava, Major Professor, Dr. Tadeusz M. Babij, and Dr. Maria Martinez for their strong support. I would also like to thank my Family , who motivated me for doing masters and has been a source of guidance, support and encouragement through out this degree program.

Thanks are also due to the High Speed Tele Networking lab members for their companionship and support. I would like to acknowledge the support I got form Electrical Engineering Department especially Pat Brammer for her support and words of encouragement.

# ABSTRACT OF THE THESIS

# MULTILINGUAL INTERACTIVE INTEGRATED MULTIMEDIA BASED E-COMMERCE

by

Amol S. Chobe

Florida International University, 2000

Miami, Florida

Professor Subbarao V. Wunnava, Major Professor

As we approach the end of the twentieth century, E-commerce is a critical force shaping the world of today and tomorrow. E-commerce have introduced a new society where people can buy freely, anywhere, at anytime, across the globe on the web. There seems to be a market for consultants and outsourcing purveyors who will take your money and put together an online business for you. These are all very different markets, however. As lot of people speak different language than English, the concept of Multilingual Technology is essential.

The primary purpose of this research paper is to study the Integrated Multimedia interaction with today's technology secondary purpose is to check out the Application of this technology in E –Commerce with the help of Multilingual technology.

Multilingual-based E-commerce would prompt more widespread use of the types of services now available and prompt the development of new and better services and the benefits brought by information, technology, and information services available will be magnified and extended globally.

TABLE OF CONTENTS

CHAPTER PAGE

# LIST OF TABLES

# LIST OF FIGURES

FIGURE PAGE

# LIST OF ACRONYMS

**Abstract**
a short summary of a journal article. Some databases include an abstract with the reference information about an article.

**Bookmarks**
a record of Web pages stored by a Web browser. Web browsers allow you to mark interesting pages by adding to a list known as a bookmark list. So when you want to return to a page you can select an item from a menu rather than typing in a URL. Bookmarks are held in a file - the location of the file is usually specified in the Options menu of the Web browser. If you are using a public lab then you should save your bookmarks on a floppy disk as you may be on a different PC when you next want to use them.

**CD-ROM**
A Compact Disc that stores digital information. CD's can store huge quantities of text, reasonable amounts of sound or still pictures and tiny amounts of moving images. CD-ROMs (Read Only Memory) are often used to store bibliographic databases.

**Citation**
A reference to a particular article

**Citation search**
A search forwards through time for all subsequent articles that have referred to the chosen article.

**BIDS**
Bath Information & Data Services
Telnet site: bids.ac.uk
Web site: `http://www.bids.ac.uk/` (not all databases can be accessed via the Web)
BIDS is a UK-based provider of bibliographic data services. It contains reference information rather than full-text information. A username and password are required - these are available from the Library. Recommended.

**Email**
a means of sending computer-readable information from one person to another.

**FAQ**
Frequently Asked Questions. An Internet term for a collection of questions and answers often asked by newcomers to a subject - particularly a newsgroup.

**First Search**
Telnet site: `fscat.oclc.org`
An online bibliographic database. Password available from the library.

**Free text Searching**
Some databases allow you to search through all the words in a record. Other databases restrict searches to certain parts such as the author or the title. Alta Vista supports free text searching of the Web.

**FTP**
file transfer protocol. FTP allows a person to transfer files between two computers, generally connected via the Internet. FTP is incorporated into Web browsers such as Netscape Navigator.

**Full-text**
a complete article or book. As opposed to a reference. Most full-text sources are on paper but increasingly you can find full-text on the World Wide Web.

**Gateway**
A intermediate computer system that allows you structured access to several other databases. BIDS is a gateway system.

**Gopher**
a fore-runner of the World Wide Web. Gopher systems appear as a list of text items. Gophers can be used by Web browsers and `gopher://` can appear at the start of a URL.

**Hierarchical indices**
Information stored in a hierarchical manner; in groups of increasingly abstract classes. To find out about emus (or whether they had anything about emus) in a hierarchical index one might go down the following index options in the hierarchy: Life sciences, Biology, Birds, Flightless Birds, Emus. Yahoo provides a hierarchical index of web pages.

**Hit**
A term for the matching of a search expression with an item in a database, e.g. "this search returned 5 hits"

**Interface**
The arrangement of things displayed by a computer. Interfaces usually consist of text, graphics, windows, menus, dialogue boxes etc.

**Internet**
a network of computers around the world. Incorporating the World Wide Web, online catalogues and many other computerized resources.

**keyword**
A word that can be used when searching for an article. Indexers may include a list of keywords along with an article. The aim is to characterize the significant elements of the article so that someone searching would use one or more of those keywords if

their interests coincided. To support this, some databases list the keywords that have been used. In databases that permit free text searching, the term keyword is also used to refer to the words that a searcher guesses might be useful in yielding the data she wants.

**Journal**
A publication consisting of articles. Journals appear in volumes, each volume having several issues (or numbers).

**Link**
a connection between two Web pages. When a link is selected on a Web page the Web browser retrieves the page at the other end of the link and displays it.

**LISTSERV**
A popular computer program that runs a mailing list.

**Lynx**
a text-only Web browser.

**Mailbase**
Web site: `http://www.mailbase.ac.uk/`
A UK centre for mailing lists.

**Mailing List**
Information distributed to its members via email.

**News, Newsgroups**
A worldwide bulletin board of electronic messages. A bit like public archived email. News requires a specialist software program to read it, e.g. Netscape Navigator. News is divided into different interest areas, e.g. talk.politics, rec.arts.disney, sci.physics etc. For detailed information see the Web site:
`http://sunsite.unc.edu/usenet-i/usenet-help.html`

**NISS**
National Information Systems and Services.
Web site: `http://www.niss.ac.uk/`
A UK site listing many online sources. Recommended.

**Online catalogue**
A computer database that gives you information on the books and journals in a library. Lancaster University Library catalogue is at:
Telnet site: `felix.lancs.ac.uk`

**Periodical**
A publication which has issues on a regular (periodic) basis. A generic term that covers newspapers, magazines, journals etc.

**Search engine**

A computer program that allows you to search a database. Often used of the search facilities for the Web. Alta Vista is a search engine for the Web.

**Search expression**

a query made to a database. It may be a particular thing such as an authors name or a book title. Very often a search expression consists of a number of keywords combined with and, or, and not.

**Serial**

A librarian's term for a journal or a periodical

**Stem**

The first part of a word or series of words. Words with the same stem are usually related, e.g. communicate, communicates, communication, communication, communicative all share the same stem of communication. A word stem is usually used together with a wildcard character to perform a truncation search. This is a searching trick to ensure you get all the articles that use the concept that the stem relates to even if they use a different word.

**Stop words**

common words removed from search expressions, e.g. *the*, *be*, *to*, *and*. There may a method of searching for these words but it varies from system to system.

**Telnet**

A program that enables you to connect to online computer systems.

**Truncation**

The removal of letters from the end of a word, or series of words. Often a word is truncated to a common stem and a wildcard character is added.

**Uncover**

An online database available via the BIDS gateway.

**Union catalogue**

a combined catalogue of several smaller catalogues. For example, COPAC is a union catalogue of several university library catalogues, as is MELVYL.

**URL**

Uniform Resource Locator. A way of identifying a Web page or other resource on the World Wide Web. All of these are valid URLs:

```
file://wuarchive.wustl.edu/mirrors/msdos/graphics/gifkit.zip
ftp://wuarchive.wustl.edu/mirrors
http://www.w3.org:80/default.html
news:alt.hypertext
telnet://dra.com
```

**Usenet**
another term for Newsgroups.

**Web browser**
A name given to a software program to access the World Wide Web. Also called a Web client or client browser. Examples are Netscape Navigator, Microsoft Explorer, NCSA Mosaic and Lynx.

**Web page**
a page of information on the World Wide Web.

**Web site**
a collection of pages on the World Wide Web. Used synonymously with Web server.

**Web server**
a computer that responds to requests from Web browsers by returning Web pages.

**WWW**
World Wide Web
A global network of computers accessed by Web browsers. Part of the Internet.

**World Wide Web Consortium**
Web site: `http://www.w3.org/`
A organization of people developing the World Wide Web.

**Wildcard, wildcard character**
A character, which stands for any other letter or letters in a search expression. A wildcard allows a search by keyword to match many related words. Wildcard characters vary between systems but most commonly the * stands for any number of letters and the? Stands for one letter. For example,

`Swim*` will match `swim, swims, swimmer, swimmers, swimming, swimmingly` etc

`swim` will match `swim` and `swam` but not `swims`

# Chapter 1. Introduction

## 1.1 Introduction

One possible definition of electronic commerce would be: "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact"[1]. However, while accurate, such a definition hardly captures the spirit of electronic commerce, which in practice is far better viewed as one of those rare cases where changing needs and new technologies come together to revolutionize the way in which business is conducted. Electronic commerce is a means of enabling and supporting such changes *on a global scale*. It enables companies to be more efficient and flexible in their internal operations, to work more closely with their suppliers, and to be more responsive to the needs and expectations of their customers. It allows companies to select the best suppliers regardless of their geographical location and to sell to a global market.

One special case of electronic commerce is *electronic trading*, in which a supplier provides goods or services to a customer in return for payment. A special case of electronic trading is *electronic retailing*, where the customer is an ordinary consumer rather than another company. However, while these special cases are of considerable economic importance, they are just particular examples of the more general case of any form of business operation or transaction conducted via electronic media. Other equally valid examples include internal transactions within a single company or provision of information to an external organization without charge.

Electronic commerce is technology for change. Companies that choose to regard it only as an "add on" to their existing ways of doing business will gain only limited benefit. The major benefits will accrue to those companies that are willing to change their organizations and business processes to fully exploit the opportunities offered by electronic commerce.

## 1.2 Building out the Internet

Where advances in telecommunications and computing largely occurred side-by-side in the past, today, they converge in the Internet. Soon, virtually all information technology investment will be part of inter-linked communications systems, whether internal to a business, between businesses, between individuals and businesses, or individual-to-individual. However measured, the Internet is expanding at a very rapid pace.

In 1994, three million people, most of them in the United States, used the Internet [2]. In 1998, 100 million people around the world use the Internet. Some experts believe that one billion people may be connected to the Internet by 2005 [3]. This expansion is driving dramatic increases in computer, software, services and communications investments.

**Table 1.1 Growths of Internet Hosts and Domain Names [6]**

| | **Number of Hosts (in millions)** | **Number of Domains (in thousands)** |
|---|---|---|
| July 93 | 1,776 | 26 |
| July 94 | 3,212 | 46 |
| July 95 | 6,642 | 120 |
| July 96 | 12,881 | 488 |
| July 97 | 19,540 | 1,301 |

* Internet host refers to a computer that is connected to the Internet that has a unique Internet Protocol (IP) address. A domain name represents a record within the Domain Name System.

**Source:** Network Wizards, http://www.nw.com

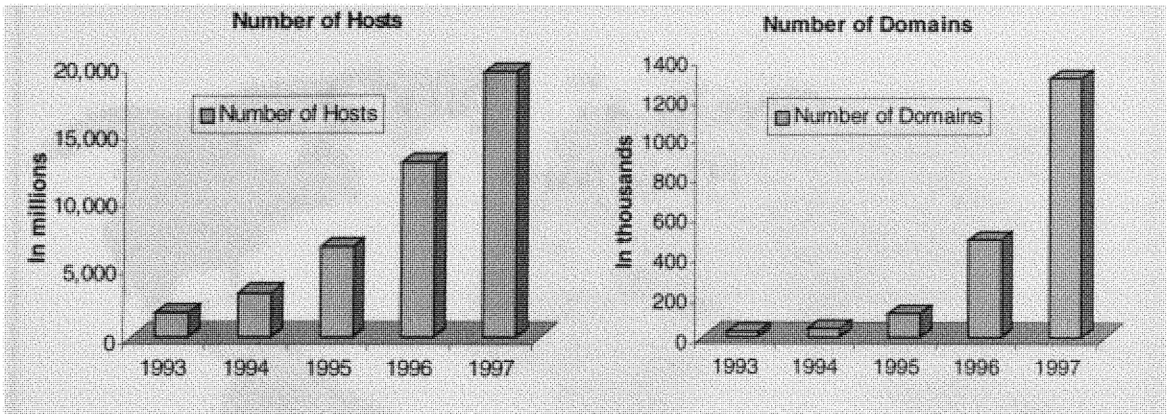


**Figure 1.1 Growth of Internet Hosts and Domain Names [4]**

For instance, the number of Americans using the Internet has grown from fewer than 5 million in 1993 to as many as 62 million by 1997 [4]. UUNET, one of the largest Internet backbone providers, estimates that Internet traffic doubles every 100 days [5]. The number of names registered in the domain name system grew from 26,000 in July 1993 to 1.3 million in four years. Over the same period, the number of hosts connected to the Internet expanded from under 1.8 million to over 19.5 million [6] (Table. 1.1).

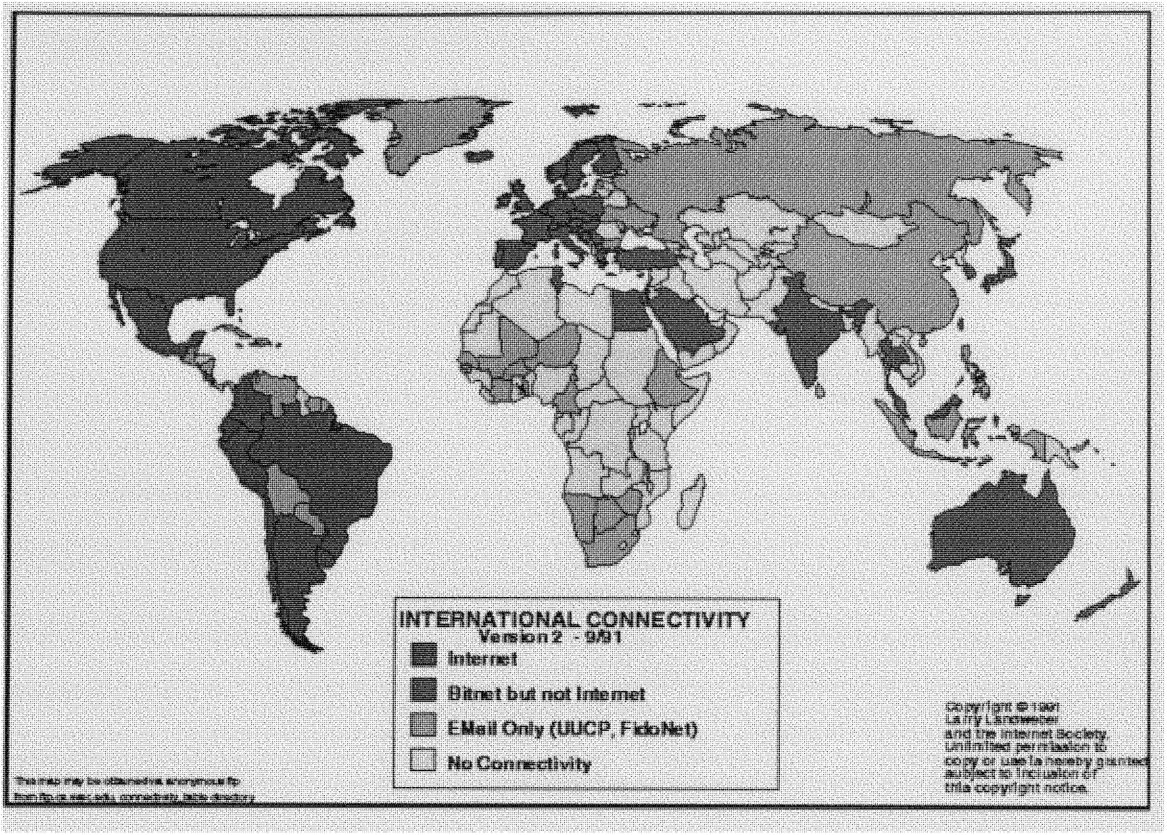

INTERNATIONAL CONNECTIVITY
Version 2 - 9/91
Internet
Bitnet but not Internet
EMail Only (UUCP, FidoNet)
No Connectivity
This map may be obtained via anonymous ftp
from ftp.cs.wisc.edu connectivity_table directory
Copyright © 1991
Larry Landweber
and the Internet Society.
Unlimited permission to
copy or use is hereby granted
subject to inclusion of
this copyright notice.

**Figure 1.2 International Internet connectivity in 1991 [4]**

Figure 1.2 illustrates the International Internet connectivity in the year 1991 and Figure 1.3 shows the same for the year 1997. Comparison between these figures clearly represents the huge growth in the global Internet connectivity.

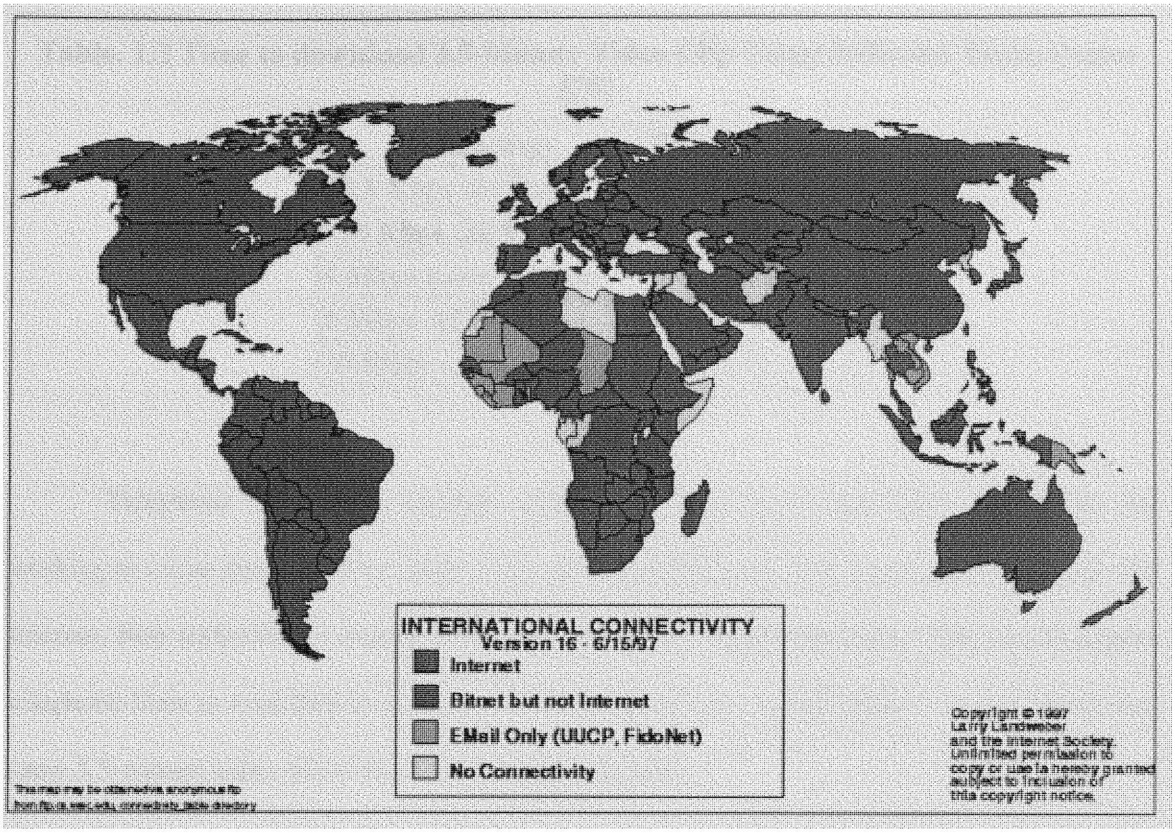

INTERNATIONAL CONNECTIVITY
Version 16 · 6/15/97
Internet
Bitnet but not Internet
EMail Only (UUCP, FidoNet)
No Connectivity
Copyright © 1997
Larry Landweber
and the Internet Society.
Unlimited permission to
copy or use is hereby granted
subject to inclusion of
this copyright notice.
This map may be obtained via anonymous ftp
from ftp.cs.wisc.edu, connectivity_table directory

Figure 1.3 International Internet connectivity in 1997 [4]

## 1.3 Making the Internet faster and More Accessible

Households typically connect to the Internet through a PC and a telephone line. This method of access means that most households without PCs (just under 60 percent of all U.S. households) [7] do not have Internet access. It also means that most Internet connections from the home are slow [8].

To illustrate the importance of speed, it takes 46 minutes to download a 3.5-minute video using a 28.8 Kbps (thousand bits per second) modem, the modem most commonly used by households today (Table. 1.2).

**Table. 1.2 Time to download 3.5-Minute Video Clip Using Different Technologies [29]**

| Technology | Transfer Time |
|---|---|
| 28.8 Kbps modem | 46 minutes |
| 128 Kbps ISDN | 10 minutes |
| 4 Mbps cable modem | 20 seconds |
| 8 Mbps ADSL | 10 seconds |
| 10 Mbps cable modem | 8 seconds |

Telephone companies, satellite companies, cable service providers and others are working to create faster Internet connections and expand the means by which users can access the Internet. New technologies such as ADSL (Asynchronous Digital Subscriber Line) enable copper telephone lines to send data at speeds up to 8 million bits per second (Mbps). At this speed, that same 3.5-minute video takes 10 seconds to download [9].

As the number of Internet users grows, accessing the Internet becomes faster and easier to do, and as the number of Internet-enabled devices multiplies, the IT industry's share of the economy can be expected to continue to expand rapidly.

## 1.4 E-commerce

E-commerce (electronic commerce or EC) is the buying and selling of goods and services on the Internet, especially the World Wide Web. In practice, this term and a new term, "e-business," are often used interchangably. For online retail selling, the term e-tailing is sometimes used. [30]

E-commerce can be divided into:

- E-tailing or "virtual storefronts" on Web sites with online catalogs, sometimes gathered into a "virtual mall"
- The gathering and use of demographic data through Web contacts

- Electronic Data Interchange (EDI), the business-to-business exchange of data
- E-mail and fax and their use as media for reaching prospects and established customers (for example, with newsletters)
- Business-to-business buying and selling
- The security of business transactions

### 1.4.1 E-tailing or The Virtual Storefront and the Virtual Mall

As a place for direct retail shopping, with its 24-hour availability, a global reach, the ability to interact and provide custom information and ordering, and multimedia prospects, the Web is rapidly becoming a multibillion dollar source of revenue for the world's businesses. A number of businesses already report considerable success. As early as the middle of 1997, Dell Computers reported orders of a million dollars a day. By early 1999, projected e-commerce revenues for business were in the billions of dollars and the stocks of companies deemed most adept at e-commerce were skyrocketing. Apart from computer and network products, books (Amazon.com), gardening products (Garden.com), music on compact disks (CDNow), and office supplies (SuppliesOnline) were a few of the better-known e-commerce sites [10]. By early 1999, even businesses that have always counted on face-to-face customer interaction were planning e-commerce Web sites and many businesses were planning how to coordinate in-store and Web store retail approaches. Meanwhile, new businesses based entirely on Web sales were being invented daily.

### 1.4.2 Market Research

In early 1999, it was widely recognized that because of the interactive nature of the Internet, companies could gather data about prospects and customers in unprecedented amounts -through site registration, questionnaires, and as part of taking orders. The issue of whether data was being collected with the knowledge and permission of market subjects had been raised. (Microsoft referred to its policy of data collection as "profiling" and a proposed standard has been developed that allows Internet users to decide who can have what personal information.)

### 1.4.3 Electronic Data Interchange (EDI)

EDI is the exchange of business data using an understood data format. It predates today's Internet. EDI involves data exchange among parties that know each other well and make arrangements for one-to-one (or point-to-point) connection, usually dial-up.

### 1.4.4 E-Mail, Fax, and Internet Telephony

E-commerce is also conducted through the more limited electronic forms of communication called e-mail, facsimile or fax, and the emerging use of telephone calls over the Internet. Most of this is business-to-business, with some companies attempting to use e-mail and fax for unsolicited ads (usually viewed as online junk mail or spam) to consumers and other business prospects. An increasing number of business Web sites offer e-mail newsletters for subscribers. A new trend is opt-in e-mail in which Web users voluntarily sign up to receive e-mail, usually sponsored or containing ads, about product categories or other subjects they are interested in.

### 1.4.5 Business-to-Business Buying and Selling

Thousands of companies that sell products to other companies have discovered that the Web provides not only a 24-hour-a-day showcase for their products but a quick way to reach the right people in a company for more information.

### 1.4.6 The Security of Business Transactions

Security includes authenticating business transactors, controlling access to resources such as Web pages for registered or selected users, encrypting communications, and, in general, ensuring the privacy and effectiveness of transactions. Among the most widely used security technologies are SSL and RSA. Secure Electronic Transactions (SET) is an emerging industry standard.

## 1.5 Multilingual Approach to E-Commerce .

E-commerce is flourishing most impressively in English-speaking countries, but a tremendous market is being missed for marketers outside of these countries, as people there are going online fast, especially in Europe. We will discuss the main factors that are responsible for the development of e-commerce in countries where other European languages are spoken besides English, and show a few examples of U.S. companies who are successful in using their Website to develop international e-commerce. My intent is to encourage the reader to look outside Anglophone countries for online export sales.

### 1.5.1 Globalization

Globalization has become the most dynamic force of our time, along with the movement to go online. The Web has helped barriers come down between countries, and there is a strong drive today to address foreign markets. Globalization has already been highly developed between Anglophone countries, thanks to a common language. But then again, there are only 6 countries where English is the mother tongue: the U.S., Canada, the U.K., Australia, New Zealand and South Africa, all told, some half a billion people.

### 1.5.2 European Languages Flourish Online

Let us understand the facts on the relative online populations in countries where

European languages are spoken (not English). According to the latest statistics (www.euromktg.com/globstats) [11], 82 million people people access the Internet from Anglophone countries, whereas 41 million people access the Internet in other European languages. This non-English figure represents astounding growth, since only 20 months ago, there were only 7 million people in this category, and now there are 41 million: nearly a six-fold growth in 20 months. (As a point of reference, Asian languages today represent 18 million people online.)

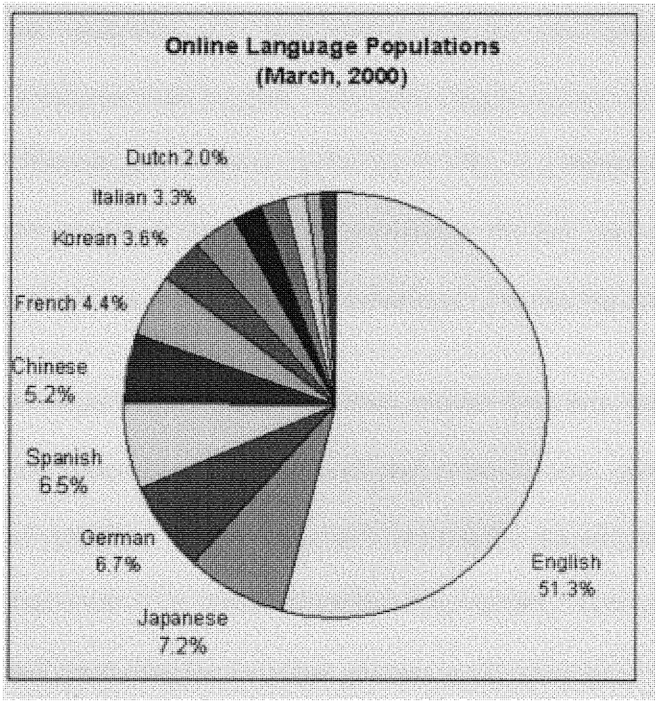


**Figure 1.4 Online language population [11]**

German-speaking Europe will be first to see strong growth of e-commerce. The Multimedia Director from top German publisher Bertelsmann recently stated that the German e-commerce market should grow to $23 B within a few years, which will represent 5% of

German retail revenues. France will follow, since the teletext system known as Minitel has been in use since 1981, and e-commerce last year saw $3.3 billion sold online (over the Minitel). (Compare this figure to the $11 billion sold by e-commerce last year... worldwide.) Indeed, 20% of the French have already purchased online, in comparison with 3% of the American population.

## 1.6 Drawing Customers to a Website

Most Websites in Anglophone countries only give information about their offering in English, and the small numbers of visitors who come from non-Anglophone countries arrive more by chance than by deliberate marketing. Most Webmasters think that other languages on their site are extraneous, since "everyone reads English": they have simply missed the entire point of what marketing is all about. Promoting a Website, marketing its URL, is a matter of communicating for the first time to unknown people, or drawing their attention to the site. And outside of Anglophone countries, English is never used to communicate a marketing message.

The best and most economical way a Website can draw visitors from non-Anglophone countries is to have a few important pages translated, and promote those "gateways" into the site, in each targeted country. A passive approach (leaving the site only in English) will yield one-fifth or one-sixth of its visitors from non-Anglophone countries. An active approach (translating and promoting the language gateways) can yield up to one-half (or more) of its visitors from non-Anglophone countries. The impact on sales is significant.

## 1.7 Case studies

At the top end of the scale there is Charles Schwab, the extremely successful online stock brokerage, with $26 billion of investments made online last year. They opened a Chinese part of their Website in May, 1998, backed up by a Chinese e-Team that is dedicated to supporting the on-line investing needs of its Chinese speaking customers.

Another success story is Dell Computers, who has translated their site into most every language. Of the daily $5 million of sales coming through their Website, $1 million comes from abroad. The proportion of international sales to total sales should grow considerably, since mature PC vendors (such as Compaq) draw two-thirds of their sales from abroad.

Cyberian Outpost is a computer ware distributor who sells only online: one-third of their sales come from outside the U.S. Historically, they had a foothold in Asia (mainly Japan) before Europe, and Japanese sales are still stronger than in Europe. They realize such a success by translating the most important four pages of their site into 9 languages (soon 12). These "language gateways" have only been registered in the large, international indexes, not the local ones in each country. However, they do advertise on Lycos (which is available in 9 languages), and this accounts for a lot of traffic from international audiences.

Spyzone sells spy equipment both online and offline. Their site uses 6 languages to introduce visitors to the company in their own language for the last two years, which has given them terrific response -- technology transfer deals, new resellers in certain countries, and lots of international sales, some quite large. In fact, more than one-third of their overall sales comes from abroad, much of it coming from people finding the Website. They registered with many foreign indexes, so people could find them if they looked for certain keywords. Banner ads are also used, as well as print advertising for their retail outlets, which includes the URL. The end result is some 400-500 email inquiries every month, and a reasonable percentage of these leads become clients.

Sportsline reports on sports news. They translated much of their site into Japanese, as well as a "gateway" page in French, German and Spanish, all of which are registered in indexes. The result is that 30-35% of their overall site traffic comes from outside the U.S., with approximately 20% of their e-commerce sales coming from international customers.

In contrast to U.S. sites, where a multilingual format is extremely rare, there are many examples of European companies successfully using a multilingual approach on their Website to build sales. Popular languages to use on these sites, besides English, are German, French, Spanish and Italian. Here are some examples of European Websites that contain several languages for wider audience:

- Kenzo (fashion)
- Damart (household appliances)
- Floritel (flowers)
- Michelin Travel (the tire company that also publishes a complete series of travel guides)
- Relais et Châteaux (top hotel chain)
- Bordeaux Wine
- Swiss Army Knives
- U.K. tire company
- Disneyland Paris

These companies have a more sophisticated approach to international marketing than their insular Anglophone cousins, and will be able to penetrate deeper into foreign markets. But that is a subject for another article.

In conclusion, I would strongly encourage taking international markets seriously in order to stay in the running. History shows that new entrants into a virgin market can often lock it up, so that it is quite difficult later on for competitors to enter. Competition is heating up very fast, and if you do not properly address foreign markets, your competitors surely will... no matter which side of the Atlantic they come from.

## 1.8 Thesis Outline

In this thesis the author will discuss a model for the E-Commerce network demonstrating techniques that may be used in the development and implementation of the same. The application has been developed using currently available tools and technologies, will also be discussed.

Chapter 2 describes the system considerations and architecture of the today's Internet network. The tasks that will be performed for the implementation of the E-commerce Site will be discussed in detail, including the different uses and applications of such information networks.

Chapter 3 discusses what is E-commerce? How its works? This chapter provides a detailed description of the different setup of the e-commerce site that were considered for the implementation of the network model. It also provides reasons as to why these particular technologies were chosen over the other existing ones.

Chapter 4 discusses the Security system that are commonly used for the E-commerce site . This Chapter will have in detail the discussion about the security system used on Internet and which one is good for our site. This Chapter mainly Focus on SSL security scheme.

Chapter 5 provides an overview Multilingual Approach to E-commerce . In this chapter we will discuss the need of multilingualism for today E-commerce site . Also , the detail of how we are going to use multilingualism technology with E-commerce site .

The concept of machine translation is also discussed in this Chapter.

Chapter 6 describes the E-commerce Site model that was developed by the author. Software tools that will be used for the development of the E-commerce site. A detailed discussion of the implementation of the E-commerce, which was proposed by the author, is provided in this chapter. It explains about real website in operation and also the steps, which should be followed before implementing this site.

Chapter 7 discusses the conclusion given by the author. The author suggests some future enhancements for the Multilingual approach to E-commerce site.

# Chapter 2. Software & Hardware tools for E-Commerce

## 2.1 Introduction

Unless you have been living under a rock for the last two years, you have heard about e-commerce! And you have heard about it from several different angles. For example:

- You have heard about all of the companies that offer e-commerce because you have been bombarded by their TV and radio ads.
- You have read all of the news stories about the shift to e-commerce and the hype that has developed around e-commerce companies.
- You have seen the huge valuations that web companies get in the stock market, even when they don't make a profit.
- And you may have actually purchased something on the web, so you have direct personal experience with e-commerce.

## 2.2 Commerce

Before we get into a complete discussion of **e-commerce**, it is helpful to have a good mental image of plain old commerce first. If you understand commerce, then e-commerce is an easy extension.

Merriam-Webster's Collegiate Dictionary defines commerce as follows:

> com.merce n [MF, fr. L commercium, fr. com- + merc-, merx merchandise] (1537) 1: social intercourse: interchange of ideas, opinions, or sentiments 2: the exchange or buying and selling of commodities on a large scale involving transportation from place to place 3: sexual intercourse

We tend to be interested in the second definition, but that third one is interesting and unexpected - maybe that's what all of the hype is about!

So commerce is, quite simply, the exchange of goods and services, usually for money. We see commerce all around us in in millions of different forms. When you buy something at a grocery store or at Wal-mart you are participating in commerce. In the same way, if you cart half of your possessions onto your front lawn for a yard sale, you are participating in commerce from a different angle. If you go to work each day for a company that produces a product, that is yet another link in the chain of commerce. When you think about commerce in these different ways, you instinctively recognize several different roles:

- Buyers - these are people with money who want to purchase a good or service.
- Sellers - these are the people who offer goods and services to buyers. Sellers are generally recognized in two different forms: **retailers** who sell directly to consumers and **wholesalers** or **distributors** who sell to retailers and other businesses.
- Producers - these are the people who create the products and services that sellers offer to buyers. A producer is always, by necessity, a seller as well. The producer sells the products produced to wholesalers, retailers or directly to the consumer.

You can see that at this high level, commerce is a fairly simple concept! Whether it is something as simple as a person making and selling popcorn on a street corner or as complex as a contractor delivering a space shuttle to NASA, all of commerce at its simplest level relies on buyers, sellers and producers.

## 2.3 The Elements of Commerce

When you get down to the actual elements of commerce and commercial transactions, things get slightly more complicated because you have to deal with the details. However, these details boil down to a finite number of steps. The following list highlights all of the elements of a typical commerce activity. In this case, the activity is the sale of some product by a retailer to a customer:

- If you would like to sell something to a customer, at the very core of the matter is the something itself. You must have a **product or service** to offer. The product can be anything from ball bearings to back rubs. You may get your products directly from a producer, or you might go through a distributor to get them, or you may produce the products yourself.
- You must also have a **place** from which to sell your products. Place can sometimes be very ephemeral - for example a phone number might be the place. If you are a customer in need of a back rub, if you call "Judy's Backrubs, Inc." on the telephone to order a back rub, and if Judy shows up at your office to give you a backrub, then the phone number is the place where you purchased this service. For most physical products we tend to think of the place as a store or shop of some sort. But if you think about it a bit more you realize that the place for any traditional mail order company is the combination of an ad or a catalog and a phone number or a mail box.
- You need to figure out a way to get people to come to your place. This process is known as **marketing**. If no one knows that your place exists, you will never sell anything. Locating your place in a busy shopping center is one way to get traffic. Sending out a mail order catalog is another. There is also advertising, word of mouth and even the guy in a chicken suit who stands by the road waving at passing cars!
- You need a way to accept **orders**. At Wal-mart this is handled by the check out line. In a mail order company the orders come in by mail or phone and are processed by employees of the company.
- You also need a way to accept **money**. If you are at Wal-mart you know that you can use cash, check or credit cards to pay for products. Business-to-business transactions often use purchase orders. Many businesses do not require you to pay for the product or service at the time of delivery, and some products and services are delivered continuously (water,

power, phone and pagers are like this). That gets into the whole area of **billing** and **collections**.

- You need a way to deliver the product or service, often known as **fulfillment**. At a store like Wal-mart fulfillment is automatic. The customer picks up the item of desire, pays for it and walks out the door. In mail-order businesses the item is packaged and mailed. Large items must be loaded onto trucks or trains and shipped.
- Sometimes customers do not like what they buy, so you need a way to accept **returns**. You may or may not charge certain fees for returns, and you may or may not require the customer to get authorization before returning anything.
- Sometimes a product breaks, so you need a way to honor warranty claims. For retailers this part of the transaction is often handled by the producer.
- Many products today are so complicated that they require **customer service** and **technical support** departments to help customers use them. Computers are a good example of this sort of product. On-going products like cell phone service may also require on-going customer service because customers want to change the service they receive over time. Traditional items (for example, a head of lettuce), generally require less support that modern electronic items. [13]

You find all of these elements in any traditional mail order company. Whether the company is selling books, consumer products, information in the form of reports and papers, or services, all of these elements come into play.

In an e-commerce sales channel you find all of these elements as well, but they change slightly. You must have the following elements to conduct e-commerce:

- A product
- A place to sell the product - in the e-commerce case a web site displays the products in some way and acts as the place

- A way to get people to come to your web site
- A way to accept orders - normally an on-line form of some sort
- A way to accept money - normally a merchant account handling credit card payments. This piece requires a secure ordering page and a connection to a bank. Or you may use more traditional billing techniques either on-line or through the mail.
- A fulfillment facility to ship products to customers (often outsource-able). In the case of software and information, however, fulfillment can occur over the Web through a file download mechanism.
- A way to accept returns
- A way to handle warrantee claims if necessary
- A way to provide customer service (often through email, on-line forms, on-line knowledge bases and FAQs, etc.)

In addition, there is often a strong desire to integrate other business functions or practices into the e-commerce offering. An extremely simple example -- you might want to be able to show the customer the exact status of an order.

### 2.3.1 Why the Hype?

There is a huge amount of hype that surrounds e-commerce. Given the similarities with mail order commerce, you may be wondering why the hype is so common. Take, for example, the following quotes from different pages

- "On the retail side alone, Forrester projects $17 billion in sales to consumers over the Internet by the year 2001. Some segments are really starting to take off." --Forrester Research, "Content and Context..," DMA Insider, Spring 1998.

- "Worldwide business access to the Web is expected to grow at an even faster rate than the US market--from 1.3 million in 1996 to 8 million by 2001." --O'Reilly & Associates
- "Home continues to be the most popular access location, with nearly 70% of users accessing from their homes...almost 60% shop online. The most popular activities include finding information about a product's price or features, checking on product selection and determining where to purchase a product." --IntelliQuest Information Group, Inc., WWITS Survey
- "In general, the more difficult and time-consuming a purchase category is, the more likely consumers will prefer to use the internet versus standard physical means." eMarketer. [14]

This sort of hype applies to a wide range of products. According to eMarketer the biggest product categories include:

- Computer products (hardware, software, accessories)
- Books
- Music
- Financial Services
- Entertainment
- Home Electronics
- Apparel
- Gifts and flowers
- Travel services
- Toys
- Tickets
- Information

### 2.3.2 The Lure of E-commerce

The following list summarizes what might be called the "lure of e-commerce" [15]:

- Lower transaction costs - if an e-commerce site is implemented well, the web can significantly lower both order-taking costs up front and customer service costs after the sale by automating processes.
- Larger purchases per transaction - Amazon offers a feature that no normal store offers. When you read the description of a book, you also can see "what other people who ordered this book also purchased". That is, you can see the related books that people are actually buying. Because of features like these it is common for people to buy more books that they might buy at a normal bookstore.
- Integration into the business cycle - A Web site that is well-integrated into the business cycle can offer customers more information than previously available. For example, if Dell tracks each computer through the manufacturing and shipping process, customers can see exactly where their order is at any time. This is what FedEx did when they introduced on-line package tracking - FedEx made far more information available to the customer.
- People can shop in different ways. Traditional mail order companies introduced the concept of shopping from home in your pajamas, and e-commerce offers this same luxury. New features that web sites offer include:
    - The ability to build an order over several days
    - The ability to configure products and see actual prices
    - The ability to easily build complicated custom orders
    - The ability to compare prices between multiple vendors easily
    - The ability to search large catalogs easily

- Larger catalogs - A company can build a catalog on the web that would never fit in an ordinary mailbox. For example, Amazon sells 3,000,000 books. Imagine trying to fit all of the information available in Amazon's database into a paper catalog!
- Improved customer interactions - With automated tools it is possible to interact with a customer in richer ways at virtually no cost. For example, the customer might get an email when the order is confirmed, when the order is shipped and after the order arrives. A happy customer is more likely to purchase something else from the company.

It is these sorts of advantages that create the buzz that surrounds e-commerce right now.

There is one final point for e-commerce that needs to be made. E-commerce allows people to create completely new business models. In a mail order company there is a high cost to printing and mailing catalogs that often end up in the trash. There is also a high cost in staffing the order-taking department that answers the phone. In e-commerce both the catalog distribution cost and the order taking cost fall toward zero. That means that it may be possible to offer products at a lower price, or to offer products that could not be offered before because of the change in cost dynamics.

However, it is important to point out that the impact of e-commerce only goes so far. Mail order sales channels offer many of these same advantages, but that does not stop your town from having a mall. The mall has social and entertainment aspects that attract people, and at the mall you can touch the product and take delivery instantly. E-commerce cannot offer any of these features. The mall is not going to go away anytime soon...

## 2.4 Easy and Hard Aspects of E-commerce

The things that are hard about e-commerce include:

- Getting traffic to come to your web site

- Getting traffic to return to your web site a second time
- Differentiating yourself from the competition
- Getting people to buy something from your web site. Having people look at your site is one thing. Getting them to actually type in their credit card numbers is another.
- Integrating an e-commerce web site with existing business data (if applicable)

There are so many web sites, and it is so easy to create a new e-commerce web site, that getting people to look at yours is the biggest problem.

The things that are easy about e-commerce, especially for small businesses and individuals, include:

- Creating the web site
- Taking the orders
- Accepting payment

## 2.5 Building an E-commerce Site

The things you need to keep in mind when thinking about building an e-commerce site include:

- Suppliers - this is no different from the concern that any normal store or mail order company has. Without good suppliers you cannot offer products.
- Your price point - a big part of e-commerce is the fact that price comparisons are extremely easy for the consumer. Your price point is important in a transparent market.
- Customer relations - E-commerce offers a variety of different ways to relate to your customer. E-mail, FAQs, knowledge bases, forums, chat rooms... Integrating these features into your e-commerce offering helps you differentiate yourself from the competition.

- The back end: fulfillment, returns, customer service - These processes make or break any retail establishment. They define, in a big way, your relationship with your customer.

When you think about e-commerce, you may also want to consider these other desirable capabilities:

- Gift-sending
- Affiliate programs
- Special Discounts
- Repeat buyer programs
- Seasonal or periodic sales

The reason why you want to keep these things in mind is because they are all difficult unless your e-commerce software supports them. If the software does support them, they are trivial.

## 2.6 Affiliate Programs

A big part of today's e-commerce landscape is the affiliate program [16] (also known as associate programs). This area was pioneered by Amazon. Amazon allows anyone to set up a specialty book store. When people buy books from the specialty store, the person who owns the specialty bookstore gets a commission (up to 15% of the book's list price) from Amazon. The affiliate program gives Amazon great exposure because hundreds of thousands of specialty bookstores popped up all over the web. Therefore this model is now copied by thousands of e-commerce sites. If you are setting up an e-commerce site you will want to consider an affiliate program as one way to get exposure. BeFree and Link Share are two companies that help e-commerce sites set up affiliate programs.

A relatively new twist on affiliate programs is the **CPC Link** (CPC=Cost Per Click), also known as affiliate links or click-thru links. You put a link on your site and the company pays you when someone clicks on the link. A typical payment ranges from 5 cents to 20 cents per click. Affiliate links represent the middle ground between banner ads and commission-based affiliate programs. With banner ads, the advertiser takes all the risk -- if no one clicks on the banner then the advertiser wastes money. Commission-based affiliate programs place all the risk on the web-site. If the web site sends a bunch of people to the affiliate e-commerce site but no one buys anything, then it has no value for the web site. In CPC links, both sides share risks and rewards equally. You may want to consider setting up this sort of affiliate program to gain exposure for your e-commerce site.

## 2.7 General Implementation of E-commerce Site

There are three general ways to implement the site with all sorts of variations in between. The three general ways are:

- Enterprise computing
- Virtual hosting services
- Simplified e-commerce

These are in order of decreasing flexibility and increasing simplicity.

**Enterprise computing** means that you purchase hardware and software and hire a staff of developers to create your e-commerce web site. Amazon, Dell and all of the other big players participate in e-commerce at the enterprise level. You might need to consider enterprise computing solutions if:

- You have immensely high traffic - millions of visitors per month

- You have a large database that holds your catalog of products (especially if the catalog is changing constantly)
- You have a complicated sales cycle that requires lots of customized forms, pricing tables, etc.
- You have other business processes already in place and you want your e-commerce offering to integrate into them.

**Virtual hosting services** give you some of the flexibility of enterprise computing, but what you get depends on the vendor. In general the vendor maintains the equipment and software and sells them in standardized packages. Part of the package includes security, and almost always a merchant account is also an option. Database access is sometimes a part of the package. You provide the web designers and developers to create and maintain your site.

**Simplified e-commerce** is what most small businesses and individuals are using to get into e-commerce. In this option the vendor provides a simplified system for creating your store. The system usually involves a set of forms that you fill out online. The vendor's software then generates all of the web pages for the store for you. Two good examples of this sort of offering include Yahoo Stores and Verio Stores .You pay a couple of hundred dollars a month for these services.

## 2.8 Types of E-commerce

Ultimately, many forward thinking business managers are now implementing advanced eBusiness solutions. These eBusiness systems can essentially be divided into two categories – Business to Business (B2B) and Business to Consumer (B2C) [17].

B2B solutions allow businesses to communicate more effectively, integrating their business processes and linking them to their suppliers, customers, partners and distributors. At present, the biggest financial gains from use of the Internet in Europe and North America are coming from B2B deals - buying and selling commodities like paper, plastics, chemicals, even livestock!

Streamlining specific inter-business processes that are time consuming, costly and inefficient can lead to significant cost savings and a quick Return on Investment (ROI). For example, many companies are looking at their communications and ordering processes used with national and overseas strategic partners and cutting the cost of complicated and inefficient paper trails by automating these processes using B2B eBusiness solutions.

Companies are thus able to work closely together by linking their enterprise applications and their systems so they can deliver products by the quickest and most cost-effective means.

B2C solutions are customer focused, are largely made up of packaged solutions (B2B solutions require more customisation), and rely more on successful marketing and a well-designed web site / user interface. They attract buyers (or merchants) by clever advertising often on other web sites. Whilst they do not generally need the capability to handle regular bulk orders, they do require high availability and efficient order fulfilment, as do B2B solutions

# Chapter 3. Web Architecture

## 3.1 How the Web Works

The World Wide Web is by far the most popular part of the Internet. Once you spend time on the Web, the graphical portion of the Internet, you will begin to feel like there is no limit to what you can do. The Web allows rich and diverse communication by displaying text, graphics, animation, photos, sound and video.

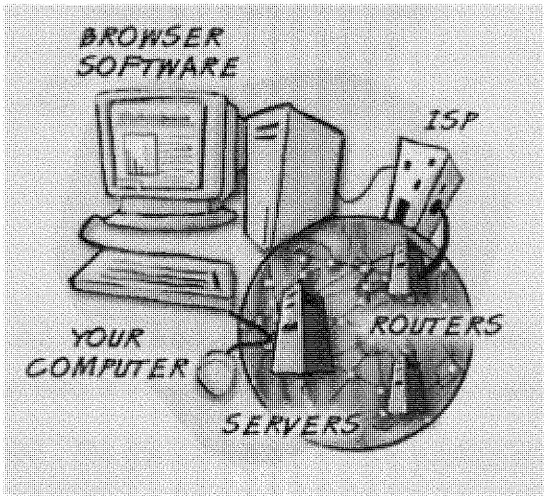
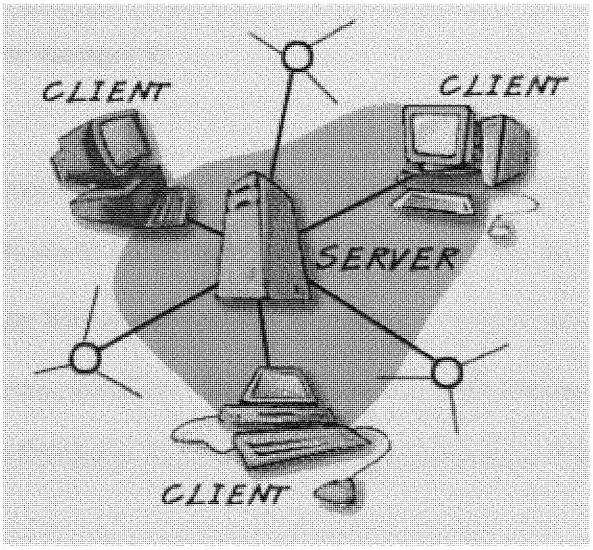


**Figure 3.1 Outline of Internet [31]**

So just what is this miraculous creation? The Web physically consists of your personal computer, web browser software, a connection to an Internet service provider, computers called servers that host digital data and routers and switches to direct the flow of information.

The Web is known as a client-server system. Your computer is the client; the remote computer that stores electronic files is the server. Here's how it works:

Let's say you want to pay a visit to the Florida International University website. First you enter the address or URL of the website in your web browser (more about this in a while). Then your browser requests the web page from a web server located in Miami. The FIU's server sends the data over the Internet to your computer. Your web browser interprets the data and displays it on your computer screen.



**3.2 Client and server relationship [31]**

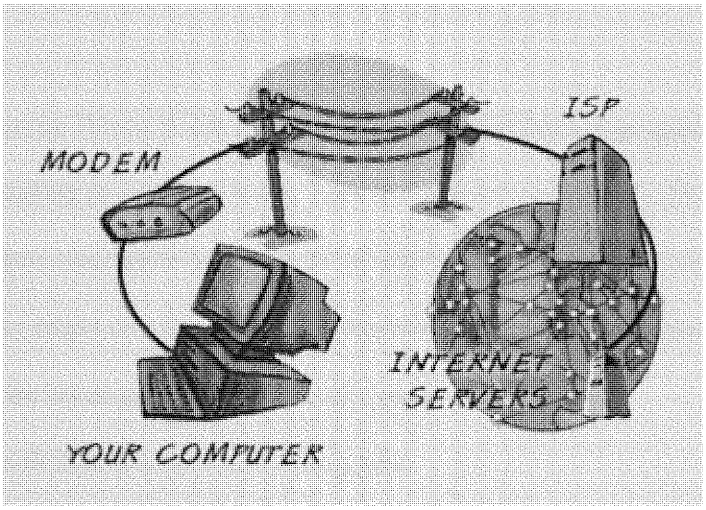
The FIU website also has links to other websites. With a click of your mouse on a link, you can access the web server in Paris . The glue that holds the Web together is called hypertext and hyperlinks. This feature allows electronic files on the Web to be linked so that you can easily jump between them. On the Web, you navigate through pages of information based on what interests you at that particular moment. This is commonly known as browsing or surfing the Net.

To access the Web you need software, such as Netscape Navigator or Microsoft Internet Explorer, known as web browsers. How does your web browser distinguish between web pages and other files on the Internet? Web pages are written in a computer language called HTML, which stands for Hypertext Markup Language.

## 3.2 Some Web History

The World Wide Web (WWW) was originally developed in 1990 at CERN, the European Laboratory for Particle Physics. The World Wide Web Consortium, also known as the World Wide Web Initiative now manages it.

The WWW Consortium is funded by a large number of corporate members, including AT&T, Adobe Systems, Inc., Microsoft Corporation and Sun Microsystems, Inc. Its purpose is to promote the growth of the Web by developing specifications and reference software that will be freely available to everyone. The Consortium is run by MIT with INRIA (The French National Institute for Research in Computer Science) acting as European host, in collaboration with CERN.



**3.3 Internet Connectivity [31]**

The National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign was instrumental in the development of early graphical software utilizing the World Wide Web features created by CERN. NCSA focuses on improving the productivity of researchers by providing software for scientific modeling, analysis, and visualization. The World Wide Web was an obvious way to fulfill that mission. NCSA Mosaic, one of the earliest web browsers, was distributed free to the public. It led directly to the phenomenal growth of the World Wide Web.

### 3.3 Anatomy of a Web Page

A web page is an electronic document written in a computer language called HTML, short for Hypertext Markup Language. Each web page has a unique address, called a URL, short for Uniform Resource Locator, which identifies its location on the network.

A website has one or more related web pages, depending on how it's designed. Web pages on a website are linked together through a system of hyperlinks, so that you can jump between them by clicking on a link. On the Web, you navigate, popularly knowing as surfing, through pages of information based on what interests you at that particular moment.

When you browse the World Wide Web you'll see the term home page quite a lot. Think of a home page as the starting point of a website. Like the table of contents of a book or magazine, the home page in most cases gives an overview of what you'll find at the website. A website can have one page, many pages or a few long ones, depending on how it's designed. If there isn't a lot of information, the home page may be the only page.

But usually you will find at least a few other pages.

Web pages vary wildly in their design and content, but most use a traditional magazine format. At the top of the page is a masthead or banner graphic. Then there's a list of items, such as articles, often with a brief description. The items in the list are usually hot, meaning that they are linked to other pages in the website or to other websites. Sometimes these links are highlighted words in the body of the text or are arranged in a list, just like an index. They can also be a combination of both. A web page can also have images that link to other content.

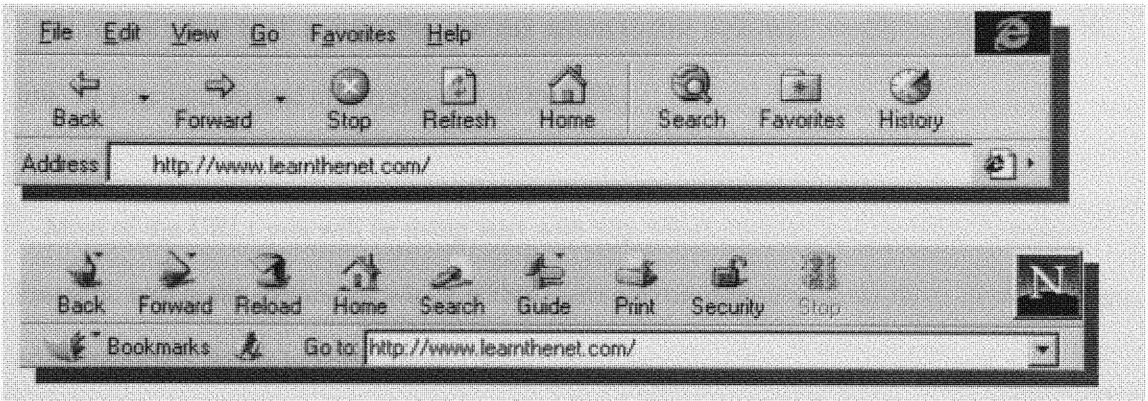
How can you tell which text are links or "hot?" Text links appear in a different olor from the rest of the text--typically blue and underlined. When you move your cursor over a text link or over a graphic link, it will change from an arrow to a hand. And by the way, the hot words often hint at what you will link to.

When you return to a page with a link you've already visited, the hypertext words will often be in a different color, so you know you've already been there. But you can certainly go there again. Don't be surprised though, if the next time you visit a site, the page looks different and the information has changed. The Web is a dynamic medium. To encourage visitors to return to a site, some web publishers change the pages often. That's what makes browsing the Web so exciting.

### 3.3.1 Understanding Web Addresses

You can think of the World Wide Web as a network of electronic files stored on computers all around the world. Hypertext links these resources together. Uniform Resource Locators or URLs are the addresses used to locate these files. The information contained in a URL gives you the ability to jump from one web page to another with just a click of your mouse. Whether you type a URL into your browser or click on a hypertext link, your browser is actually sending a request to download a file stored on a remote computer.

The first part of a URL (before the two slashes) tells you the type of resource or method of access at that address. For example:



Address http://www.learnthenet.com/

Go to http://www.learnthenet.com/

**3.4 web bars [32]**

http - a hypertext document or directory

gopher - a gopher document or menu

ftp - a file available for downloading or a directory of such files

news - a newsgroup

telnet - a computer system that you can log into over the Internet

WAIS - a database or document in a Wide Area Information Search database

file - a file located on a local drive (your hard drive)

The second part of a URL is typically the address of the computer where the data or service is located. Additional parts may specify the names of files, the port to connect to, or the text to search for in a database.

You can enter the URL of a site by typing it into the Location window of your web browser, just under the toolbar.

Most browsers can record URLs that you want to use again, by adding them to a special menu. In Netscape Navigator, it's called Bookmarks. In Microsoft Explorer, it's called Favorites.

Once you add a URL to your list, you can return to that web page simply by clicking on the link in your list, instead of retyping the entire URL.

Most of the URLs you will be using start with http which stands for Hypertext Transfer Protocol. http is the method by which HTML files are transferred over the Web. Here are some other important things to know about URLs:

1.A URL usually has no spaces.

2.A URL always uses forward slashes.

3.If you enter a URL incorrectly, your browser will not be able to locate the site or resource you want. If you get an error message or the wrong site, make sure you typed the address correctly.

4.You can find the URL behind any link by passing your mouse cursor over the link. The pointer will turn into a hand and the URL will appear in the browser's status bar, usually located at the bottom of your screen.

### 3.4 Under the Hood of the World Wide Web

Driving a web browser or other computer application is as easy as driving a car -- or at least it should be. "You don't have to know how the computer works, just how to work the computer." This article is a quick peek "under the hood", one level deeper, to give you some idea what's going on behind the scenes.

The story of web browsers and web sites builds up from many different parts to a grand finale. Here are the parts...

- **Client/Server Concepts**
- **Internet Concepts**
- **Port Numbers**
- **Protocols**
- **Domain Names**
- **Mark-up Languages**
- **What's a URL?**
- **Bitmapped Graphics**
- **Putting it All Together**
- **Going Even Further**

### 3.4.1 Client/Server Concepts

A client computer initiates a service request. A server computer waits to reply, kind of like a person who waits to answer the phone so you can make airline reservations.

A client program can be directed by a human being (at a screen, keyboard, and mouse), or it can run automatically.

A server is a program that knows a protocol for communication (see below), but often doesn't know much about networking -- it just exchanges bytes of information with the client, a back-and-forth conversation that might be human-readable ASCII, or binary code; kind of like when you call someone to make a reservation, and they don't know how the phone system works, just how to use the telephone to talk with you.

It's entirely possible for the client and server programs to be on the same computer, as well as on two different computers connected by a network. The client/server model blurs the boundaries between computers, to where "the network IS the computer."

Once a virtual connection is established between a client and server, the two systems are peers, but the client/server asymmetry usually continues through the protocol; just like when you're done dialing someone, it doesn't matter much who placed the call, you can talk to each other as equals, though quite often the caller and the caller have very different roles. (With phone calls the caller usually pays for any long distance charges, but there's usually no equivalent in network connections.) [18]

### 3.4.2 Internet Concepts

A TCP/IP network is a common connection between two or more computers. The connection is often through coaxial cable (coax), the same sort of stuff that's used for TV antenna signals, but it doesn't have to be. Network connections can be made by radio, infra-red light, carrier pigeon, you name it. Nowadays it's more common to see UTP (unshielded twisted pair) wiring, which is "star shaped" from a central hub out to each system; and the hubs talk with each other over fiber-optic cable.

A network connection is shared by every computer on the same Local Area Net (LAN). They can all hear each other; imagine a bunch of people standing in a small room together.

Only one network host (computer) on a LAN can talk at a time and be understood, unless the arrangement is something like UTP, where the hub can route traffic just between the interested parties. [18]

A networked computer talks by sending a packet of data (a series of bits/bytes) addressed to either one other computer, (normal TCP/IP) or to everyone on the LAN who's listening (often UDP/IP).

Everyone on the LAN takes turns talking. On coax, if two computers start to talk at the same time, there's a protocol for deciding who gets to talk when. You can imagine a bunch of people in a discussion group, except most of the time they're talking to just one other person and the rest of the people aren't listening (until their name is called). On UTP, any pair of people can whisper to each other without bothering others in the room who are doing the same thing.

### 3.4.3 Hardware addresses

Every networked computer has at least one LAN interface (card) that contains a world-wide unique hardware address set by the manufacturer (48 bits = 6 bytes long). They look like this: 080009352D52.

You can think of hardware addresses as being like the numbers on the wires that leave the local phone company to go to your home telephone. You don't usually

deal with them, but they are necessary to route your calls.

Hardware addresses are assigned to manufacturers in blocks of numbers at a time.

A network interface's hardware (station) address is only known to the other computers on the local network.

Two computers talking on a local network actually address each other by hardware address. [18].

### 3.4.4 Gateways

Local networks are connected by gateways, which are either general-purpose or dedicated computers that are connected to two or more different LANs or WANs (wide area networks). They know which data packets should be forwarded from one network to another. Imagine two groups of people in two adjacent rooms, with one person at the common door who passes messages between the rooms. Separate conversations can take place in each room at the same time, but messages can also be relayed between the rooms. [19]

### 3.4.5 IP addresses

Every LAN interface is assigned a world-wide unique IP address (32 bits = 4 bytes). You can think of this address as the interface's "phone number". IP addresses look like this: 15.1.50.9.

IP addresses are assigned to companies as blocks of subnet addresses. For example, HP owns net 15, and also some parts of net 192 such as 192.6.40.

Since a computer can have more than one LAN interface, it can have more than one IP address (phone number) -- just like your house. [19]

### 3.4.6 Hostnames and routes

We associate "hostnames" with IP addresses, just like we associate human or business names with phone numbers. (See below about domain names.)

Since a computer can have more than one LAN interface and IP address, it can have more than one hostname, just like people can be addressed in different ways, depending on their roles and relationships. However, each LAN interface does not necessarily have a different name, because that could be confusing.

When a client computer connects to a server computer, it looks up the server's domain name in a directory through a nameserver (see below) to find the server computer's IP address, and then figures out a route to that address by using routing services on the same system or on other systems, including a gateway.

A simple form of a route is: "To reach any machine not on the local net, go through the gateway at 15.1.50.1." The client addresses a data packet to that gateway (using the gateway's hardware address). The gateway in turn figures out how to send the packet one step closer to the intended destination on a different LAN.

When a connection request (data packet) reaches a gateway on the same LAN as the target server, the gateway talks to the server using the server's hardware address, since it knows that number. (If it doesn't, it can use ARP (address resolution protocol) to find out, kind of like a waiter in a restaurant announcing, "phone call for Mr. Liu.") [19]

### 3.4.7 Port Numbers

Once a client computer reaches (connects to) a server over the network, it needs a way to tell the server which service (server program) it wants to talk with. It does this by specifying a port number (at least in TCP/IP). You can think of port numbers as telephone extensions. Every call to a server system reaches an "operator" who asks for an extension number to put the call through.

On a server, when each server program starts running, it attaches to one or more port numbers and receives traffic on those ports. On a client, when a service is needed, the client program looks up the standard port number for the service before connecting to the server system. It's also possible for a human talking with the client system to specify the port number to use for a given connection. For example, you can "telnet" to a server's email or HTTP port and do useful things, since those services speak ASCII (not binary).

Obviously there is a lot of agreement in the world about standard port numbers, or clients would never be able to find their servers! But in fact any server computer can attach any server programs it likes to any port numbers. [18]

### 3.4.8 Protocols

Just like in real life, a computer protocol is a formal description of how to talk to (or interact with) someone else.

TCP/IP stands for "transmission control protocol / internet protocol". Along with other protocols, it describes the way that virtual connections are made over networks, including hardware addresses, IP addresses, hostnames, etc.

Once a connection is made between a client and a server, how they talk with each other is described by a service protocol. For example, FTP (file transfer protocol) is a simple language for asking a server to get and send back to the client all the bytes in a specified file.

As you can see, to carry on a conversation, a whole stack of protocols happens at the same time. It's just like if you make a phone call to a business. There's a protocol you don't know about (because you can ignore it) that says how to build and wire up telephones. There's a higher level protocol (that you do know) about how to dial phone numbers. And once you get through, there is an even higher-level protocol for how you might make a reservation or leave a message for someone.

When you call someone on the phone, you're talking to a human (or to an answering machine that will be heard by a human). Humans are pretty flexible and interactive, so you don't have to be real precise about protocols. But computer services are not so smart, so you must know and obey the protocols to talk with them. [19]

### 3.4.9 Domain Names

Domains are a way of dividing up the world of computers so each one can have a unique name (that includes its location in the network) that's easy for people to use because it's made of words, not numbers.

Each domain can contain (know about) subdomains or individual computers. A computer's full domain name starts with its hostname and ends with its top level domain. For example: "ajs.fc.hp.com" is a computer ("ajs", named for its owner) that lives in Fort Collins, Colorado ("fc") on an HP computer network ("hp"), which is a kind of commercial network ("com").

You can think of domain names as being like postal addresses -- name, apartment, street, city, state, country.

Just like there are lots of different kinds of mail addresses, there are lots of different kinds of domain addresses. They're all of the form of words separated by dots, but the meanings of the first words in the name depend on which domain they're in, that is, which words appear later in the domain name.

Just like you can have both a street address and a post office box, a computer can be in different domains at the same time, although for various reasons this isn't very common.

### 3.4.10 Name servers

Every domain or subdomain has at least one computer running a "nameserver" program, on a "well known port number", that can do name lookup. For example, if a client program on a computer named "jlk.co.edu" wants to talk with a service on server machine "ajs.fc.com", the steps work like this:

The client program on jlk.co.edu tells the computer system (jlk) it wants to make the connection. jlk looks at "ajs.fc.com". Since it doesn't know anything about this address, it asks a world-wide top-level nameserver (at a known address) for the address of "ajs.fc.com". It gets the IP address of a nameserver for "com". jlk asks the "com" server if it knows "ajs.fc.com". jlk gets an IP address for the nameserver for the "fc.com" subdomain. jlk asks the "fc.com" server if it knows "ajs.fc.com". jlk gets an IP address for that system. Now jlk connects to ajs by its IP address.

Suppose the client on jlk was a mailer (mail program) that wanted to send email to a person named "ajs" on the computer named "ajs". It would connect to the mail server's port (normally port 25), and say that it had mail for "ajs@ajs.fc.com".

Note that while jlk might talk to a number of different systems in order to send the email, the letter itself would go directly to the destination system (across some patchwork of internet segments and gateways).

If the client was trying to send mail to "ajs@fc.hp.com", a computer named hpfcla.fc.hp.com might "take the call." It would say, "I know how to reach ajs@fc.hp.com" (who's really on ajs@ajs.fc.hp.com). hpfcla would accept the letter from jlk, then connect with ajs.fc.hp.com and forward it. This is especially common when the source system can't talk directly to the destination system because it's behind a "firewall", as described later.

### 3.4.11 Mark-up Languages

A computer file is a series of bytes, usually in a code like ASCII that represents text (letters and digits), like English text.

When the text is simply lines of words, and each line ends with an ASCII "newline" character, we call that "flat ASCII".

A long time ago people realized that computers could be used to do document and book preparation. They are great at storing and manipulating text, and with printers they can print that text on paper.

"Flat ASCII" text is pretty flat-looking. Documents and books have lots of fancy features like layout, pagination, different fonts, chapter headings, drawings, etc. So people developed what are called "mark-up languages." These are ways of writing text intermingled with various formatting control commands that affect how the text is displayed or printed. For example, I might do something \fIlike this\fR to make some words appear in italics and the words after them return to normal (Roman) font.

### 3.4.12 Viewing and editing

Once you have a document that is marked up in some way, you can view it two different ways. You can edit it as flat ASCII and hand-modify the formatting control commands, or you can view or print the document "pretty printed" so you can see what the control commands do.

Nowadays most mark-up languages are supported by WYSIWYG ("what you see is what you get" or "whizzywig") editors that let you edit the document in a for similar to how it will look when it's displayed or printed by the reader. You never need to see the control codes, but you have to know a language for talking with the editor about fancy features!

Often a WYSIWYG editor will let you "view the source" of the document so you can see the complicated control language.

Computers don't have to stop with pretty-printed words. It's possible for them to display pictures and symbols mixed with the words. Some of the symbols or words can even be made active, so when you "click on them" with a mouse, something happens.

### 3.4.13 Hyperlinks

One useful action is called a "hyperlink". This is a way of changing the display to show you a different document, or a different place in the current document.

Pictures and words can both be made into hyperlinks. Text that is marked up to include hyperlinks is called "hypertext". Here's an example that shows you the control codes:

```
<A HREF="#URL">Click here</A> to page-align the following table of contents.
<a name="URL">First entry</a>...
```

This means, turn "Click here" into a hyperlink with a hidden reference of "#URL", and if I click on it, move me down to the next paragraph (after the "<P>"), at "First entry...", which has a hidden name of "URL".

The "language" called HTML (hypertext mark-up language) is the common basis of the World Wide Web. Millions of HTML documents are stored on millions of networked computers. The example above is a simple little bit of HTML.

Currently, most people who write HTML documents edit flat ASCII forms of the documents, and then view them with a Web browser to see how they look formatted.

This is kind of like writing software and then compiling it and running it to see how it works.

### 3.4.14 What's a Universal Resource Locator ?

A Universal Resource Locator (URL) is a fancy name for a line of text that uniquely specifies a resource worldwide. A resource is usually, but not necessarily, a computer file.

A URL starts with the name of a server or service; for example:

ftp:

http:

The first service is FTP, the file transfer protocol you read about earlier. The second service is HTTP, "hypertext transfer protocol". It's a simple way to ask HTTP servers for HTML documents!

(By convention, the FTP server always listens on port 21 on a server system, while the HTTP server lives on port 80.)

Normally the resource (text or image file) you want to access (view) is not on your own system, so the next piece of the URL is the domain name of the system where it lives; for example:

http://ajs.fc.hp.com

The exact form of the URL depends on the type of service! For HTTP, the next piece is a path to the file, usually relative to the "home directory" for the HTTP server; for example:

http://ajs.fc.hp.com/images/Megan.gif

This means to return an image (graphics interchange language) file that lives in the HTTP home location under images/Megan.gif.

Finally, HTTP understands that after this part of the URL there can be a wide range of other symbols that aren't a file path name, but which carry information about the service request; such as the ticker symbol for a stock whose price to look up and return.

One of the cool things about URLs is that you don't have to keep local copies of documents. They only live at the source (on the source system), and any time you need to see them, you retrieve (download) a copy of the latest version – assuming the server system is awake and you can reach it! In the past, people shared around many copies of on-line documents, and they developed elaborate schemes to try to ensure the latest copies were always distributed to all users.

But you should know that most web browsers "cache" local copies of files for a while. If you visit a website (URL) and return to it, often the return is pretty fast because a temporary local copy of the file is used. The only reason you need to know this is so it doesn't surprise you, and so you know what the "reload" button does for you.

### 3.4.15 Bitmapped Graphics

Once upon a time, to talk with a computer you had to press or flip switches and watch lights. Later people figured out how to build mechanical "teletypes" that were like typewriters, except the computer listened to your key presses and typed a reply to you on paper.

Later still, people figured out how to have computers display text and simple symbols on CRTs (cathode ray tubes, like TV sets but not exactly the same).

And even later, people figured out that computers didn't have to just display lines of text on these display screens. They could address individual bits on the screen to draw pictures, do all sorts of different sizes and fonts of text, etc. They could even put up "windows" that each acted like a separate physical display.

Along with bitmapped displays came new and different kinds of input devices than keyboards, such as mice and trackballs. With these "pointing devices" it was possible to "point and click" on a screen, choosing actions from "menus" instead of having to type "commands" to get things done.

### 3.4.16 Putting it All Together

In the early 1990s all this technology -- client/server, internet, domain names, markup languages, and graphical displays -- began to come together. People were starting to store lots of documents, marked up in various ways for pretty-printing, on networked computers, and running application programs that used windowed, graphical (bitmapped) displays and point-and-click interfaces.

Some people at CERN in Switzerland put together a markup language (HTML) with computer networking (client/server) and a new kind of server and protocol (HTTP), and with some new window-oriented, graphical, point-and-click software on the client side (a browser), to create the beginnings of the World Wide Web. Things really got going around 1993.

The Web grew like wildfire! Within just a few years, millions of documents had been created or converted to HTML and made available through HTTP servers. A variety of different web browsers (client-side programs) like Mosaic and Netscape were created and improved.

So what exactly is the World Wide Web? It doesn't really exist! It's "just" a collection of networked computers, internet connections, services and servers with lots of marked-up documents and pictures to share, and client-side browsers with which to view them. But when you put them all together, it's magic! The Web seems to have tangible substance.

What's a "homepage"? It's just an HTML document that is brought up by default when you connect to a particular server for HTTP. Often there are lots of homepages available through one server, say, one for each user on the computer. You specify which one (whose homepage) you want, as part of the URL; for example: http://udltools.fc.hp.com/~ajs is a way of retrieving the homepage for user "ajs" from the HTTP server on "udltools". Homepages are usually starting places for following hyperlinks to details about a person or organization.

Suppose someone emails you a URL. "Check out this cool website/homepage." What can you do?

You can cut and paste the URL (on your local graphical, window-smart display, using a mouse) into a data entry form provided by the web browser, say, Netscape, on your display screen.

Netscape figures out from the URL that the protocol is HTTP; then as a Client program, it asks the local computer to connect it to the domain name (computer) specified in the URL.

Along the way, if necessary, the client system looks up the IP address of the server computer from nameservers After reaching the server system, the client system asks for the HTTP server by port number.

Then it tells the HTTP server program the rest of the gibberish in the URL.
Some time later the server responds with an HTML document (or with an error). This document is shipped back over the net to your web browser, and the connection is broken. (HTTP is

"stateless", that is, it doesn't maintaina long-term relationship between the client and server. Each time the client needs something from the server, it makes a new, independent request.

However, often times the new request includes saved information based on the previous request, such as form filled out by the user.)

The client-side web browser (Netscape) "pretty prints" this HTML document and displays it on the screen for you.

All of this takes place in just a few seconds. How long, depends on how busy are the network(s) between your client system and the server system, how busy are the two systems themselves, and how much data is to be transferred. (A picture might be worth a thousand words, but it's often worth a hundred thousand bytes.)

## 3.5 Going Even Further

Much of the time a website's URL is of the common form: http://www.whatever.com and when people talk about the website, they leave off the "http://" part, or even all but the "whatever" part. Bear in mind that this is rather like giving a phone number without the area code.

Many computer networks are behind "firewalls". This means the computers in the organization can talk to each other and can connect to computers outside the firewall, but outside computers can't make inbound connections. This is why, for example, you can't reach some of the URLs I quoted above, from outside of HP.

Remember that automatic programs, not just people running programs, can be network clients. What happens when you write a "robot" that follows all the links it can, throughout the

Web, and remembers in a database the URLs and titles and documents it's seen? You get a "web search engine", like the ones at:

http://www.altavista.digital.com

http://searcher.fc.hp.com/arachnophilia (HP-internal)

You can tell these servers some words, and they locate all the web pages they know about that contain those words. Then they create (very fast, while you wait) a new, customized web page (HTML document) that includes hyperlinks to the other web pages that contain the words you wanted to find. Click! Off you go!

Most web browsers also have a way for you to record favorite URLs and their document titles, as "bookmarks" or "hotlists".

Remember that there is a protocol for every networked service... And there are lots of different kinds of computer services in common use. Guess what – most web browsers know lots of protocols! They can not only talk HTTP/HTML, they can also talk FTP (bring back and display files for you), send and receive email, and read and post netnews. That is, they can be clients for a lot of different servers, presenting them all to you, the user, through a common style of graphical display.

The three most common types of computer services, which people get confused, are these:

1.Electronic mail (email), exchanged using SMTP (simple mail transfer protocol) or other protocols. This is good for point-to-point communications, and for "broadcasting" using "mailing lists" or "mail reflectors" to lists of people. To send someone email, you need their email address, which is usually of this form:

username@domain

Conversations by email are slower and less interruptive than by telephone, but can be more precise, more easily shared widely, more easily saved and reused, etc. Email combines features of both paper mail and telephones.

2.Netnews (formerly called Usenet), exchanged using NNTP (network news transfer protocol) or other protocols. This is like a public bulletin board where anyone passing by can read what's on the board, tack up their own sheet of paper, and even send email to people who posted other notices. To achieve some sanity, old notices are automatically "taken down" (removed by the computer); discussions are grouped into "newsgroups" and then into "threads" (common titles or subjects) within each newsgroup.

Newsgroups are great for widely sharing information, especially if it is periodic in nature, like a newsletter, or is well suited for group discussion and debate. However, people often forget that all they see locally is a COPY of the bulletin board, with whatever "sheets of paper" have been copied and posted locally (to their system, or to a local news server system).
There are delays, postings can get out of order, etc.

# Chapter 4. Security of the Site

## 4.1 Introduction

The security of Internet has come more and more important. Companies and private persons are dependent that their computers that are connected to networks are working and information is confident. Security is highly depended on users and administrations as well

.

### 4.1.1 Security classification

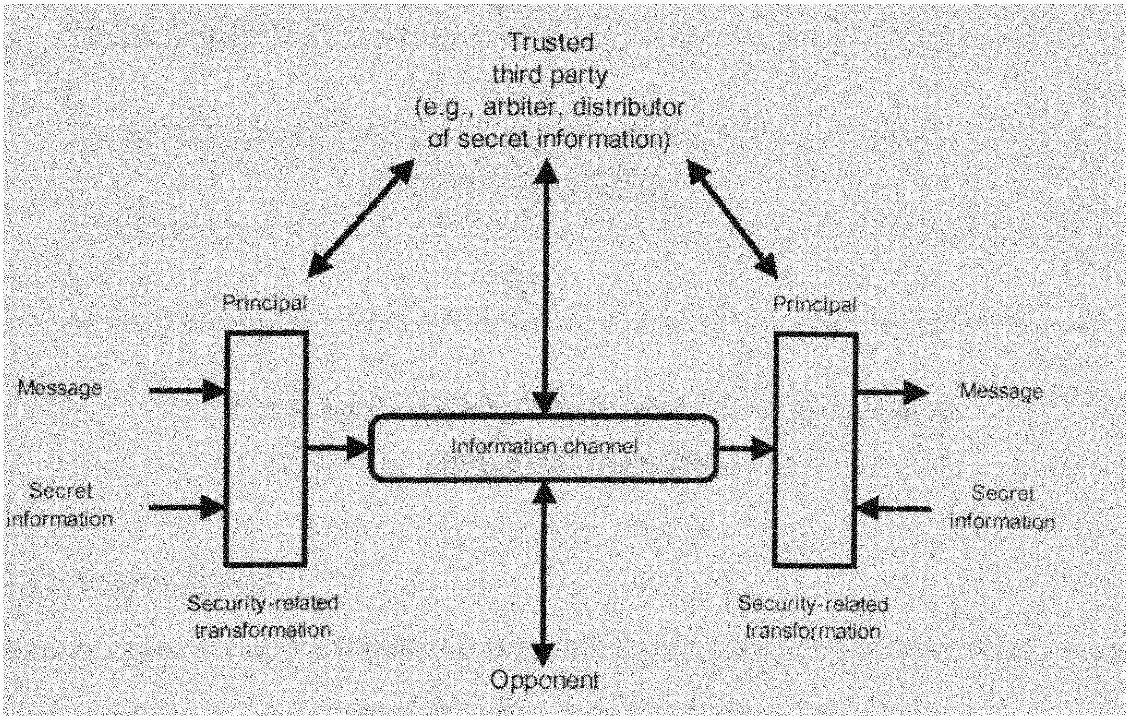
Security can be classified by many ways but one way to classify is Internet Engineering Task Force's (IETF) list:

- Confidentiality: Only authorized parties can access to information.
- Authentication: The parties that are using information (sending, receiving, etc) can be identified.
- Integrity: only authorized parties modify Information.
- Non-repudiation: Neither the sender nor receiver of message is able to deny the transmission.
- Access control: The use of target computer can be controlled. Controlling includes that user can access only to information, which is user is authorised.
- Availability: Information must be available to authorized parties when needed. This is the most difficult requirement for security systems. [20]

### 4.1.2 Methods to gain security in Internet

Security can be carried out by many means. It can be implemented in all layers of transportation. This study covers some most used methods. The Internet is complicate and in some ways uncontrolled environment. This causes that; it is the easiest way to protect the information transportation is implement the concealment in the endpoints of connection. The endpoints are the only spots that the sender and receiver can secure. Nevertheless more security can be gained also in the net.. Trusted third party scheme is coming more and more important when it's needed to have non-reputation for large number of users. Trusted Third Party must be trusted by sender and receiver. Trusted party infrastructure is shown in figure 4.1.

Public key is certificate from trusted third party, which is set available for other users. User itself can have different key for signature and encrypting.

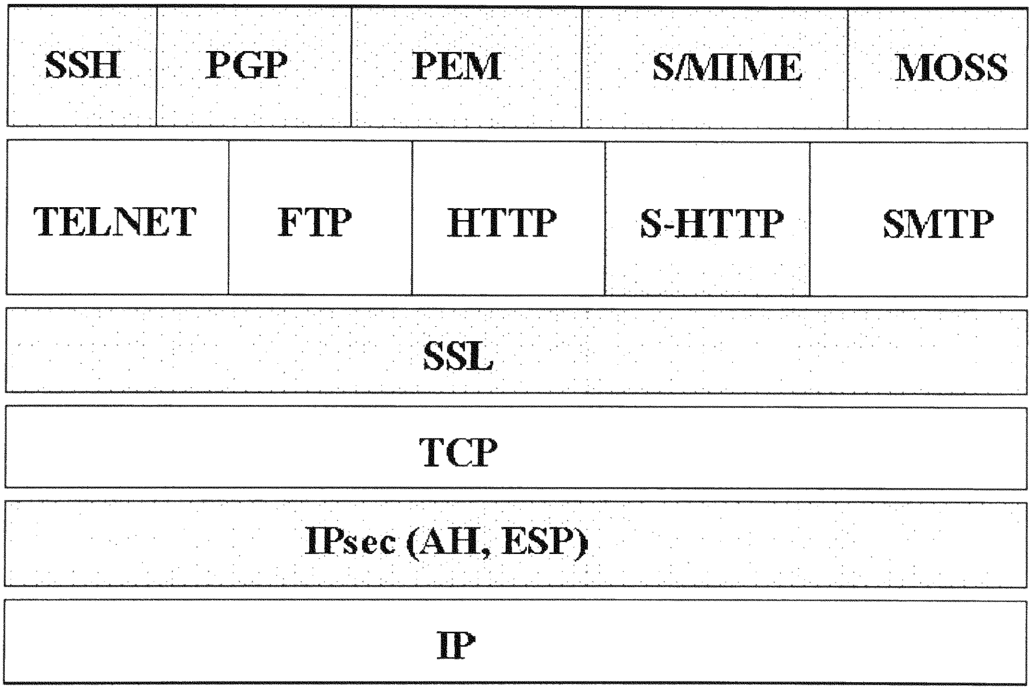


**4.1 Trusted third party infrastructure. [33]**

Encryption can be done in:

- Internet layer ( IP)
- Transportation layer ( TCP)
- Application layer

Figure 4.2 represents how the security can be gained in different layer.

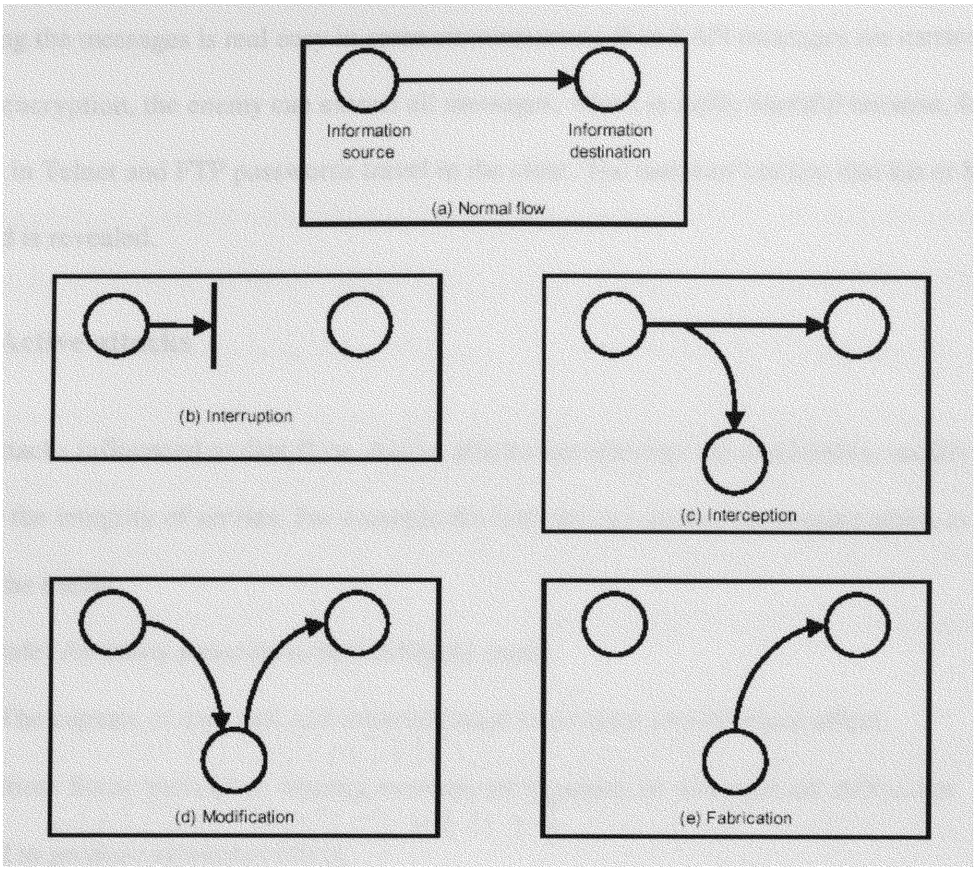


**4.2 This figure represents how security can be gained in different layers. [33]**

### 4.1.3 Security attacks

Security can be threaded with passive or active attacks. They can be represented in many ways.

Following figure 4.3 shows threats. Only the picture c represents passive attack.



**4.3 This figure represents security threats. [33]**

### 4.1.3.1 Passive attacks

Passive attacks are more difficult to detect than active. Passive attacks do not influence directly to data flow. There are two types of passive attacks: traffic analysis and finding out the content of message. Traffic analysis is almost impossible to avoid if messages are carried though commercial Internet. At least the endpoints of messages can been seen.

Traffic analysis is more useful than intuition might first exhibit. It can be used to analyze, if two companies are trading large number of messages, which might conclude in right situation that they are really discussing a merger. In future analyses can be certainly used to estimate Competitors Internet commerce.

Extracting the messages is real easy in some circumstances. If in LAN messages are carried without encryption, the enemy can extract all messages, which is really harmful because, for example in Telnet and FTP passwords travel in the clear. The user can't notice that his or her password is revealed.

### 4.1.3.2 Active attacks

Active attacks influenced to data flow. Active attacks can interrupt the availability, modify or fabricate the integrity of service. For example the intruder can modify the routing tables to redirect the traffic.

Masquerade: An entity pretends to be a different entity.

Replay: The capture of data unit and retransmission to produce unauthorized effect.

Modification: Some parts of an original message are changed, or messages are delayed or reordered to produce unwanted effect.

Denial of service: Normal use or management of service is disturbed. The messages can be suppressed or another way to degrade the service is overloading or disabling the network.

The denial of services can be caused by E-mail bombing. Bombing can be executed with various ways: sending non-stopping long messages with large, binary attachments, sending mails with forged addresses to newsgroups.

Another way to cause denial of service is TCP SYN flooding. In TCP SYN attack a large number of SYN messages are sent server to flood its buffer.

## 4.2 Cryptography

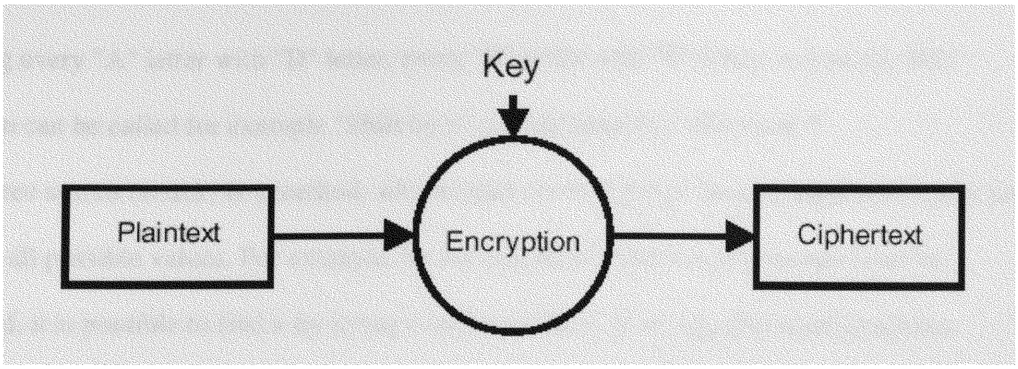
### 4.2.1 Introduction

A word cryptology is an old term that was used already by ancient creeks. Word itself consists of two parts, the first one is "krypton", which means hidden and the second one is "logos", which means word. The cryptology is an old method and it was used already by Julius Caesar to secure his communication. It consists of cryptography and cryptanalysis. Cryptography consists of the study and the practice of encryption and decryption of data, so those specific targets can only access it. These kinds of systems are called as cryptosystems. A definition of cryptography is not so straightforward and depending on source, it may vary (e.g., which is part of cryptography and which is not).

A cryptanalysis is the study and the practice of how to compromise cryptography mechanisms (cryptosystems), e.g., how to decrypt a ciphertext without a key, which is encrypted using DES-algorithm. A source data that is in understandable format (either for human or for some program) and which will be the input of cryptosystem is called plaintext (or cleantext).

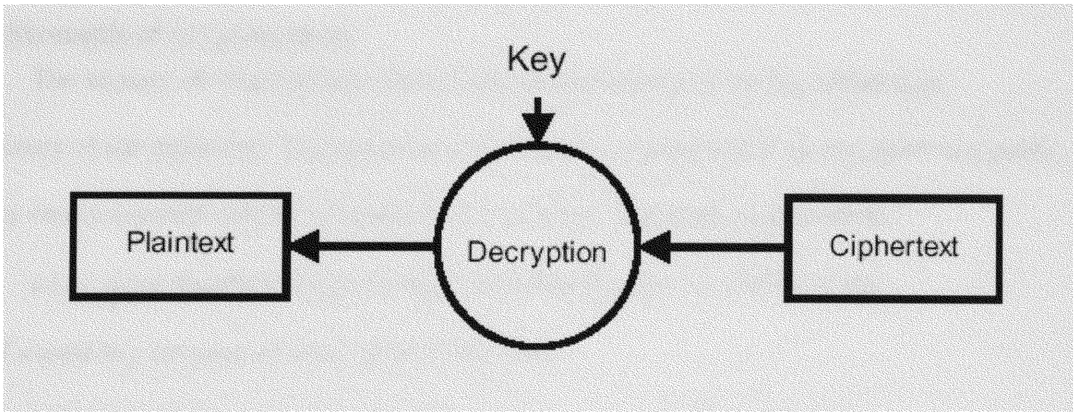
A destination data that is in non-understandable format and which will be the output of cryptosystem is called ciphertext.

Encryption is a mathematical method that transforms a plaintext to a ciphertext. Figure 4.4 represents basic encryption scheme.



**4.4 This figure represents basic encryption scheme. [33]**

Decryption is inverse method compared with encryption. Figure 4.5 represents basic decryption scheme. A key is a parameter of encryption/decryption. However, a modern cryptography is more than just an encoding and decoding data. Authentication, digital signatures and digital timestamps are also a part of modern cryptography.



**4.5 This figure represents basic decryption scheme. [33]**

Encryption algorithms have usually keys and each ciphertext has its own key. Only using a correct key can decrypt this ciphertext. For example, when Julius Caesar encrypted his data by replacing every "A" letter with "D" letter, every "B" letter with "E" letter, and so on. This algorithm can be called for example "Shift by n" and the used key value was 3.

Brute-force search (attack) is a method, which relies on computers' processing power and it just generate all possible values. For example, let say that *f(x)=y* and *y* is known and *f* can be computed, it is possible to find x by trying every possible x. If we use this method against travelling salesman problem, it simply generates all possible routes and compares the distances. This solution will work and it is simple to implement, but at the same time it is not the most efficient. (Travelling salesman problem: Given a set of towns and the distances between them, determine the shortest path starting from a given town, passing through all the other towns and returning to the first town.)

### 4.2.2 Strength of cryptosystem

- The secrecy of cryptosystem should rely on the secrecy of the key rather than the secrecy of the algorithm. A cryptosystem should be so strong that if an algorithm is a public, secrecy can be reached only by keeping secrecy of a key. (Strength of algorithm)
- a key space should be large enough which has straight correlation to the size of a used key (number of bits). (Size of the key)
- a strength of algorithm has a reverse correlation to a number of backdoors of algorithm (backdoor means that based on ciphertext it is possible to find out used key). These backdoors can be seen always as a security risk. The existence of these backdoors might be a one reason why sources of some algorithm are not public and products, which use these kinds of algorithms, may not be the most secure products available. (Possible backdoors of algorithm)

a cryptosystem should be resistant against all known attacks method. This is an important thing while designing a new cryptosystem. But also sometimes an existing cryptosystem might need upgrading because some.

new attack method is appeared and if it is known that our system does not resist that attack.

If our cryptosystem fulfils all these features mentioned above, is it strong enough? Sometimes it can be proved mathematically that a particular cryptosystem is secure, but not in all cases. What is secure enough, depends on our needs. What is the lifetime of data to be secured (2 hours, 1 week, 3 years)?

How confidential secured data is and how harmful is if secured data is revealed? It is noticeable that the cryptosystem that is secure today may not be secure after 5 years. This is partly because computers are developing so fast that year after year a cost of single operation of processor is cheaper and cheaper. For example, if a brute-force attack is impractical against our cryptosystem today, after 5 years a breaking of our system might be a piece of cake using same attack method.

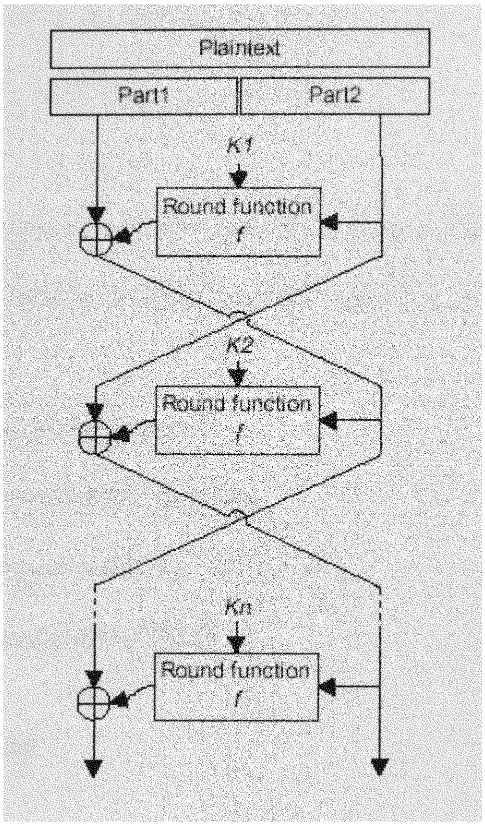
**Table 4.1. This table represents time required for exhaustive key search**. [33]

**Key Size Number of**

| **Key Size** | **Number of Alternative Keys** | **One Encryption /µs** | **$10^6$ Encryption /µs** |
|---|---|---|---|
| 32 bits | $2^{32=}4.3 * 10^{9}$ | $2^{31}$ µs=35.8 minutes | 2.15 ms |
| 56 bits | $2^{56}$=7.2 * $10^{16}$ | $2^{55}$ µs=1142 years | 10.01 h |
| 128 bits | $2^{128}$ =3.4 *$10^{38}$ | $2^{127}$ µs= 5.4 * $10^{24}$ | 5.4 * $10^{18}$ years |

## 4.3 Cipher

A cipher is part of an algorithm and is it's cryptographic "core". A block cipher is a symmetric cipher and it encrypts a block of data, size of block might vary, at the time and then goes on to the next block, and so on (e.g., RSA). A product cipher is a block cipher, which iterates a several weak operations (substitution, transposition, modular addition/multiplication and linear transformation) and Shannon introduced it at the first time 3 . Examples of modern product chippers are LUCIFER 4 and DES 5 . Feistel cipher (sometimes called DES-like cipher) is a sub-class of product cipher and they can be recognise that they operate on one half of the ciphertext at each round and then swap the ciphertext halves after each round.



**4.6 This figure represents functionality of Feistel cipher. [33]**

A following table 4.2 represents the main parameters of some product cipher:

**Table 4.2 Main parameters of some product cipher [33]**

| Cipher | Block length | key size | Number of Rounds |
|---|---|---|---|
| LUCIFER | 128 | 64 | 16 |
| DES | 64 | 56 | 16 |
| IDEA | 64 | 128 | 8 |

## 4.4 Transport Layer Security Protocols

Transport layer security protocol tries provide secure communications over unsecured communication channels. The most famous secure transport layer protocols are secure shell (SSH) and secure sockets layer (SSL).

### 4.4.1 Secure Shell

Secure shell (SSH) utilises generic transport security protocol. SSH provides the authentication of both end of connection. Integrity and confidentiality of data is protected. Data can also be compressed.

SSH consists from three major components.

- Transport layer protocol (SSH-TRANS)
- User authentication protocol (SSH-USERAUTH)
- Connection protocol (SSH-CONN)

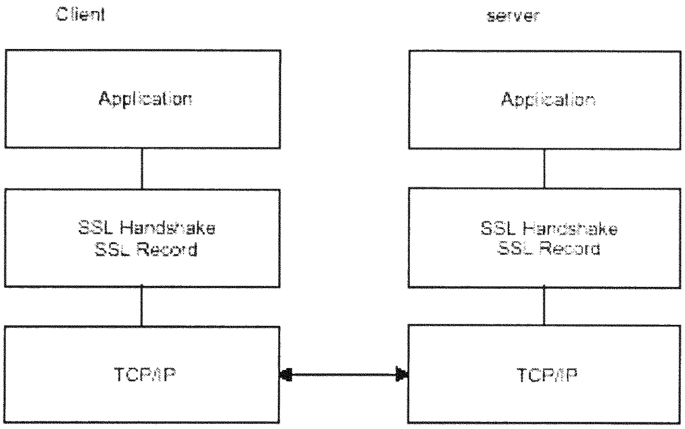
### 4.4.2 Secure Socket Layer

SSL (Secure Socket Layer) is the method proposed by Netscape Communications Corporation. It is used to encrypt transactions in higher-level protocols such as HTTP, NNTP and FTP. SSL is supported by several different browsers, including Netscape Navigator, and Microsoft Internet Explorer and many different servers, including ones from Netscape, Microsoft, IBM, Quarterdeck, OpenMarket and O'Reilly and Associates. SSL is nowadays the most supported security protocol in Internet. One big problem is that most of SSL programs have been developed in USA and Canada, that means that outside North America these products use weak keys for encrypting.

The SSL protocol provides:

- server authentication
- encryption of data in transit
- optional client authentication

SSL works between TCP/IP and application. To enable use of SSL the server and client must know that they using it (SSL). It can be done by specific port numbers for every application (hhtps 443,sssmtt 465, snntp 563, sldap 636, and spop3 995); application itself negotiates it as part of protocol or use TCP option for negotiation. SSL includes SSL record protocol and SSL handshake protocol. Figure 4.7 is representation of SSL between TCP/IP and application.

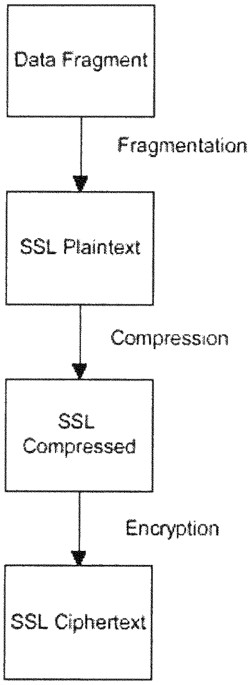


**4.7 representation of SSL between TCP/IP and application. [33]**

### 4.4.3 SSL record protocol

SSL record protocol does the fragmentation, compression, authentication and encryption for data. It puts data to SSL records, which contain: the content type (higher level protocol), version of protocol (SSL), length, data payload and message authentication code.

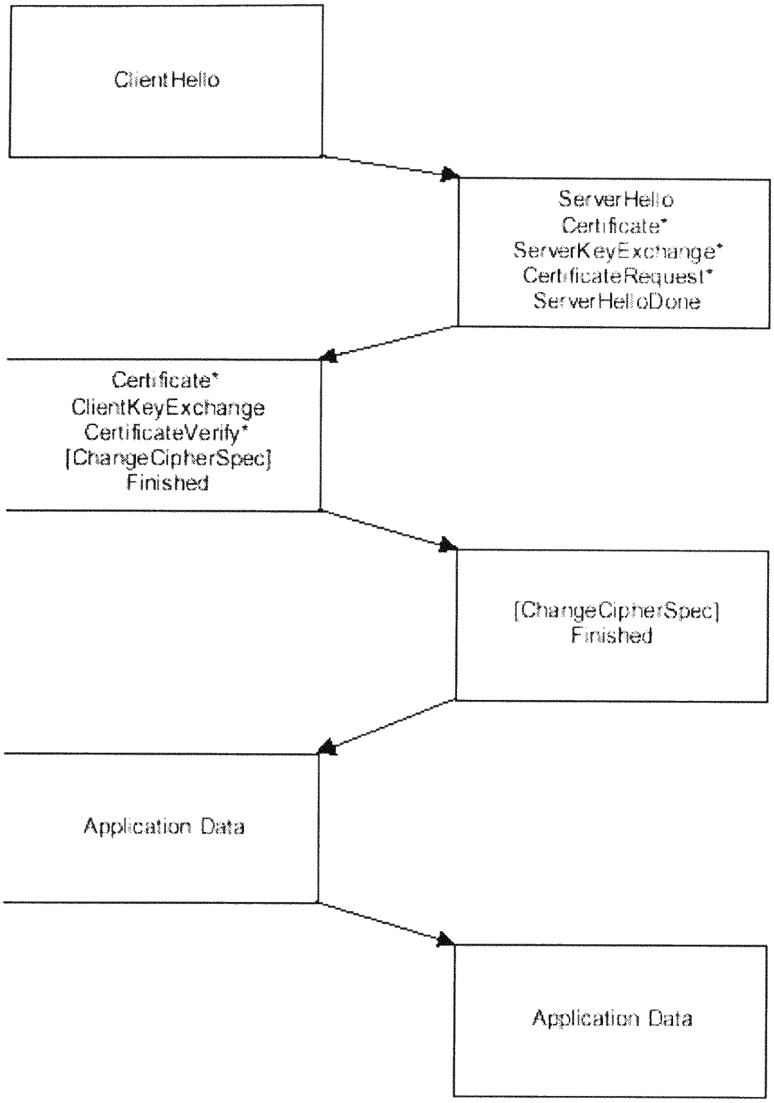
There can be several protocols above SSL record protocol as alert protocol, handshake protocol, and change cipher specification protocol. Figure 4.8 represents SSL record protocol.



**4.8 This figure represents SSL record protocol in short. [33]**

### 4.4.4 SSL Handshake Protocol

The SSL Handshake Protocol produces cryptographic parameters of the session state.



**4.9 Representation of SSL handshake protocol [33]**

The client hello and server hello messages are used to establish security Enhancement capabilities between client and server. The basic SSL handshake protocol is as shown in the figure 4.9. The client hello and server hello messages establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. First client sends hello message to server. Next step is that server send as many messages as needed to define its certificate (if it is authenticated) and client, a server key exchange and other parameters If .needed. At the end of this step server sends message to indicate that step is over. The server will then wait for a client response.

In next step client sends a change cipher spec message and then immediately sends the finished message. The server will send its own change cipher spec message its finished message. Next step is that the client and server may begin to exchange application layer data.

## 4.4 How SSL Works

### 4.4.1 An Introduction To Key Cryptography

This section explains how Netscape uses RSA public key cryptography for Internet security. Netscape's implementation of the Secure Sockets Layer (SSL) protocol employs the techniques discussed in this section. [21]

RSA public key cryptography is widely used for authentication and encryption in the computer industry. Netscape has licensed RSA public key cryptography from RSA Data Security Inc. for use in its products, specifically for authentication.

Public key encryption is a technique that uses a pair of asymmetric keys for encryption and decryption. Each pair of keys consists of a public key and a private key. The public key is made public by distributing it widely. The private key is never distributed; it is always kept secret. Data that is encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. This asymmetry is the property that makes public key cryptography so useful.

### 4.4.2 Using Public Key Cryptography For Authentication

Authentication is the process of verifying identity so that one entity can be sure that another entity is who it claims to be. In the following example involving Alice and Bob, public key cryptography is easily used to verify identity. The notation `{something} key` means that `something` has been encrypted or decrypted using `key`.

Suppose Alice wants to authenticate Bob. Bob has a pair of keys, one public and one private. Bob discloses to Alice his public key (the way he does this is discussed later). Alice then generates a random message and sends it to Bob:

| | |
|---|---|
| `A->B` | `random-message` |

Bob uses his private key to encrypt the message and returns the encrypted version to Alice:

| | |
|---|---|
| `B->A` | `{random-message}bobs-private-key` |

Alice receives this message and decrypts it by using Bob's previously published public key. She compares the decrypted message with the one she originally sent to Bob; if they match, she knows she's talking to Bob. An imposter presumably wouldn't know Bob's private key and would therefore be unable to properly encrypt the random message for Alice to check.

**BUT WAIT, THERE'S MORE**

Unless you know exactly what you are encrypting, it is never a good idea to encrypt something with your private key and then send it to somebody else. This is because the encrypted value can be used against you (remember, only you could have done the encryption because only you have the private key).

So, instead of encrypting the original message sent by Alice, Bob constructs a message digest and encrypts that. A message digest is derived from the random message in a way that has the following useful properties:

- The digest is difficult to reverse. Someone trying to impersonate Bob couldn't get the original message back from the digest.
- An impersonator would have a hard time finding a different message that computed to the same digest value.

By using a digest, Bob can protect himself. He computes the digest of the random message sent by Alice and then encrypts the result. He sends the encrypted digest back to Alice. Alice can compute the same digest and authenticate Bob by decrypting Bob's message and comparing values.

## GETTING CLOSER

The technique just described is known as a digital signature. Bob has signed a message generated by Alice, and in doing so he has taken a step that is just about as dangerous as encrypting a random value originated by Alice. Consequently, our authentication protocol needs one more twist: some (or all) of the data needs to be originated by Bob.

```
A->B        hello, are you bob?
B->A        Alice, This Is bob
            { digest[Alice, This Is Bob]
            } bobs-private-key
```

When he uses this protocol, Bob knows what message he is sending to Alice, and he doesn't mind signing it. He sends the unencrypted version of the message first, "Alice, This Is Bob." Then he sends the digested-encrypted version second. Alice can easily verify that Bob is Bob, and Bob hasn't signed anything he doesn't want to.

## HANDING OUT PUBLIC KEYS

How does Bob hand out his public key in a trustworthy way? Let's say the authentication protocol looks like this:

```
A->B        hello

B->A        Hi, I'm Bob, bobs-public-key

A->B        prove it

B->A        Alice, This Is bob

            { digest[Alice, This Is Bob]

            } bobs-private-key
```

With this protocol, anybody can be Bob. All you need is a public and private key. You lie to Alice and say you are Bob, and then you provide your public key instead of Bob's. Then you prove it by encrypting something with the private key you have, and Alice can't tell you're not Bob.

To solve this problem, the standards community has invented an object called a certificate. A certificate has the following content:

- The certificate issuer's name
- The entity for whom the certificate is being issued (aka the subject)
- The public key of the subject
- Some time stamps

The certificate is signed using the certificate issuer's private key. Everybody knows the certificate issuer's public key (that is, the certificate issuer has a certificate, and so on...). Certificates are a standard way of binding a public key to a name.

By using this certificate technology, everybody can examine Bob's certificate to see whether it's been forged. Assuming that Bob keeps tight control of his private key and that it really is Bob who gets the certificate, then all is well. Here is the amended protocol:

```
A->B        hello

B->A        Hi, I'm Bob, bobs-
```

```
A->B        certificate

B->A        prove it

            Alice, This Is bob

            { digest[Alice, This Is Bob]

            } bobs-private-key
```

Now when Alice receives Bob's first message, she can examine the certificate, check the signature (as above, using a digest and public key decryption), and then check the subject (that is, Bob's name) and see that it is indeed Bob. She can then trust that the public key is Bob's public key and request Bob to prove his identity. Bob goes through the same process as before, making a message digest of his design and then responding to Alice with a signed version of it. Alice can verify Bob's message digest by using the public key taken from the certificate and checking the result.

A bad guy - let's call him Mallet - can do the following:

```
A->M          hello

M->A          Hi, I'm Bob, bobs-

A->M          certificate

M->A          prove it

              ????
```

But Mallet can't satisfy Alice in the final message. Mallet doesn't have Bob's private key, so he can't construct a message that Alice will believe came from Bob.

**EXCHANGING A SECRET**

Once Alice has authenticated Bob, she can do another thing - she can send Bob a message that only Bob can decode:

```
                {secret}bobs-
A->B
                public-key
```

The only way to find the secret is by decrypting the above message with Bob's private key. Exchanging a secret is another powerful way of using public key cryptography. Even if the communication between Alice and Bob is being observed, nobody but Bob can get the secret. This technique strengthens Internet security by using the secret as another key, but this time it's a key to a symmetric cryptographic algorithm (such as DES, RC4, or IDEA). Alice knows the secret because she generated it before sending it to Bob. Bob knows the secret because Bob has the private key and can decrypt Alice's message. Because they both know the secret, they can both initialize a symmetric cipher algorithm and then start sending messages encrypted with it. Here is a revised protocol:

```
A->B      hello
B->A      Hi, I'm Bob, bobs-
A->B      certificate
B->A      prove it
A->B      Alice, This Is bob
B->A      { digest[Alice, This Is Bob]
          } bobs-private-key
          ok bob, here is a secret
          {secret} bobs-public-key
          {some message}secret-key
```

How `secret-key` is computed is up to the protocol being defined, but it could simply be a copy of `secret`.

### YOU SAID WHAT?

Mallet's bag contains a few more tricks. Although Mallet can't discover the secret that Alice and Bob have exchanged, he can interfere in their conversation by damaging it. For example, if Mallet is sitting between Alice and Bob, he can choose to pass most information back and forth unchanged but mangle certain messages (easy for him to do because he knows the protocol that Alice and Bob are speaking):

```
A->M        hello
M->B        hello
B->M        Hi, I'm Bob, bobs-
M->A        certificate
A->M        Hi, I'm Bob, bobs-
M->B        certificate
B->M        prove it
M->A        prove it
            Alice, This Is bob
A->M        { digest[Alice, This Is Bob]
M->B        } bobs-private-key
B->M        Alice, This Is bob
M->A        { digest[Alice, This Is Bob]
            } bobs-private-key
            ok bob, here is a secret
            {secret} bobs-public-key
            ok bob, here is a secret
            {secret} bobs-public-key
            {some message}secret-key
            Garble[ {some
            message}secret-key ]
```

Mallet passes the data through without modification until Alice and Bob share a secret. Then Mallet gets in the way by garbling Bob's message to Alice. By this point Alice trusts Bob, so she may believe the garbled message and try to act on it. Note that Mallet doesn't know the secret - all he can do is damage the data encrypted with the secret key. Depending on the protocol, Mallet may not produce a valid message. Then again, he may get lucky.

To prevent this kind of damage, Alice and Bob can introduce a message authentication code (MAC) into their protocol. A MAC is a piece of data that is computed by using a secret and some transmitted data. The digest algorithm described above has just the right properties for building a MAC function that can defend against Mallet:

```
MAC := Digest[
 some message,
      secret ]
```

Because Mallet doesn't know the secret, he can't compute the right value for the digest. Even if Mallet randomly garbles messages, his chance of success is small if the digest data is large. For example, by using MD5 (a good cryptographic digest algorithm invented by RSA), Alice and Bob can send 128-bit MAC values with their messages. The odds of Mallet's guessing the right MAC are approximately 1 in 18,446,744,073,709,551,616 - for all practical purposes, never.

Here is the sample protocol, revised yet again:

```
A->B      hello
B->A      Hi, I'm Bob, bobs-
A->B      certificate
B->A      prove it
          Alice, This Is bob
          { digest[Alice, This Is Bob]
          } bobs-private-key
          ok bob, here is a secret
          {secret} bobs-public-key
```

```
{some message,MAC}secret-key
```

Mallet is in trouble now. He can garble messages all he wants, but the MAC computations will reveal him for the fraud he is. Alice or Bob can discover the bogus MAC value and stop talking. Mallet can no longer put words in Bob's mouth.

**WHEN WAS THAT SAID?**

Last but not least to protect against is Mallet the Parrot. If Mallet is recording conversations, he may not understand them but he can replay them. In fact, Mallet can do some really nasty things sitting between Alice and Bob. The solution is to introduce random elements from both sides of the conversation.

## 4.5 Certificate

This document describes how Netscape products work with certificates when using the SSL 2.0 protocol. The document is intended to provide Certificate Authority (CA) service providers with enough details to build a service that can issue certificates for Netscape products.

### 4.6.1 How Netscape Products use SSL 2.0 Certificates

Netscape Commerce Server 1.x uses a single X.509 certificate that enables the server to authenticate itself to clients requesting SSL 2.0 connections.

When a server presents a certificate during an SSL handshake, Netscape Navigator checks the certificate against its certificate database. If the server certificate is already in Navigator's database, or if the server certificate is signed by a Certificate Authority whose certificate is in Navigator's database, the SSL handshake can conclude successfully.

Navigator 2.0 allows end users to add new trusted certificates to Navigator's certificate database. To see a list of the trusted certificates shipped with Navigator, choose Security Preferences on the Options menu. If necessary, click on the Site Certificates tab.

Navigator can handle two kinds of certificates:

1. A **Certificate Authority certificate** is a signed certificate that identifies a Certificate Authority. Netscape recommends that these certificates be self-signed. When server certificates signed by this Certificate Authority are presented during an SSL handshake, Navigator trusts those certificates. Navigator can download (via HTTP) new trusted CA certificates because they are identified by a newly defined MIME type.
2. A **site certificate** is a server certificate presented by a server during an SSL handshake. If the certificate is signed by some Certificate Authority that Navigator does not trust (that is, it does not show up on the Certificate Authority list in the Security Options dialog box or is marked by the user as not trusted), Navigator displays a series of screens that allow the user to accept or reject the certificate. (In the case of a bad certificate, Navigator displays a warning that allows the user to continue or abort the connection.)

When Navigator receives a certificate it does not already trust, it launches a wizard to guide the user through the process of installing the certificate, as follows:

1. The first time Navigator attempts to connect to an SSL server that presents a certificate Navigator does not trust, Navigator launches a wizard to install the certificate. The inital screen of the installation wizard alerts the user that Navigator has received an unrecognized certificate. The exact text on this introductory screen depends on whether the certificate is a site certificate or a Certificate Authority certificate.
2. The wizard presents human-readable information about the certificate, including the following information:
    - The organization that owns the certificate.

- The Certificate Authority that signed the certificate.
- The type of encryption (for example, Export Grade RC4, 40-bit secret key).

3. The user may choose to view more information about the certificate by clicking on the More Info button. Clicking this button opens a window that displays more information about the certificate, including:
   - Details about the organization maintaining the server (taken from fields of the subject's Distinguished Name), including the common name (CN=), organization name (O=), and country (C=).
   - The same details about the Certificate Authority.
   - Certificate serial number, validity period, and fingerprint (which is an MD5 hash of the certificate).
4. The user then chooses whether to trust this certificate.
   - **Site certificates.** Users may choose to trust the certificate for this session, trust the certificate permanently, or not to trust the certificate.
   - **Certificate Authority certificates.** Users may choose to trust or not trust CA certificates.
5. The wizard asks the user if he or she would like to be warned each time the user attempts to send data to this server. The default behavior is to display no warnings.
6. (Only for Certificate Authorities) Finally, the wizard prompts the user to enter a nickname to identify the Certificate Authority. This name appears in the list of certificates displayed in Security Preferences (on the Options menu).

   In future releases of Navigator, Netscape plans to display simply the Certificate Authority's Common Name. Therefore, Netscape encourages Certificate Authorities to use a Common Name that the user will recognize as the Certificate Authority. For example, a Common Name of "Netscape Certificate Authority" would be better than simply "Certificate Authority."

### 4.6.2 Site Certificates

The following section describe the mandatory and recommended certificate content. The content of site certificates and CA certificates are nearly identical, although there are small differences in the subject.commonName field, described below.

#### Key length of signature

All Certificate Authorities should use 1024-bit RSA keys for signing certificates. Navigator 2.0 cannot operate on keys larger than 1024 bits.

#### Certificate serial numbers

Certificate serial numbers should be unique. No Certificate Authority should issue two certificates with the same serial number.

#### Distinguished Name

The Distinguished Name of a certificate should be unique unless the same subject has several certificates issued by the same Certificate Authority (that is, owns several key pairs that need to be certified by the same CA).

#### Site certificate Certificate Info fields

The following are the mandatory or recommended values for the fields of the certificateInfo for an SSL 2.0 server certificate.

**Table 4.3 Mandatory or recommended values for the fields of the certificate Info [21]**

| **Field** | Value | Required | Comment |
|---|---|---|---|
| Version | 0 | Required | X509v1 |
| Signature | Md2 With RSA Encryption<br>Md5 With RSA Encryption | Md5 is recommended | From PKCS #1 |
| Subject Public Key Info. Algorithm | RSA  Encryption | Required | From PKCS #1 |
| Subject. Common Name | See below | Host name pattern required avoiding user seeing a warning dialog box. See below. | |

## Signature algorithm

Use of md5WithRSAEncryption is recommended. The MD2 algorithm is currently supported, but in January 1996, RSA began recommending that vendors cease using MD2 due to a potential new weakness found in the algorithm. Consequently, support for MD2 will be discontinued in a future release.

## Subject Common Name

The subject.commonName field should contain a pattern (such as *.netscape.com) that matches the DNS name of the host with which the client is connecting (such as home.netscape.com). Encoding a host name in this field is used to defeat a potential man-in-the-middle attack.

Navigator 2.0 checks the name referenced or typed by the user (the URL displayed in Navigator's Location field) against the pattern in the subject.commonName field. Note that Navigator does *not* check the result of a double-reverse-DNS lookup on the name.

Navigator 2.0 applies the following matching rules to the pattern in the subject.commonName field:

- * matches anything.
- ? matches one character.
- \ will escape a special character.
- $ matches the end of the string.
- **[abc]** matches one occurrence of **a**, **b**, or **c**. The only character that needs to be escaped in this is ]; all others are not special.
- **[a-z]** matches any character between **a** and **z**.
- **[^az]** matches any character except **a** or **z**.
- ~ followed by another shell expression will remove any pattern matching the shell expression from the match list.
- **(foo|bar)** will match either the substring **foo**, or the substring **bar**. These can be shell expressions as well.

### 4.6.3 Certificate Authority Certificates

**Key length of signature**

All Certificate Authorities should use 1024-bit RSA keys for signing certificates. Navigator 2.0 cannot operate on keys larger than 1024 bits.

**Certificate serial numbers**

Certificate serial numbers should be unique. No Certificate Authority should issue two certificates with the same serial number.

### Certificate fingerprint

Navigator calculates a certificate fingerprint that the user sees when he or she chooses Edit Certificate from the Security Options menu. This fingerprint is an MD5 hash of the certificate. Netscape encourages Certificate Authorities to publish the fingerprint for their certificate so that users may, if they desire, verify that they have the correct certificate.

### Certificate Authority Certificate Info fields

The following are the mandatory or recommended values for the fields of the certificate Info for a Certificate Authority certificate that can be downloaded to Navigator 2.0:

**Table 4.4 Certificate Authority certificate mandatory or recommended values [21]**

| **Field** | Value | Required | Comment |
|---|---|---|---|
| Signature | Md2 With RSA Encryption<br>Md5 With RSA Encryption | Required | From PKCS #1 |
| Subject Public Key Info. Algorithm | RSA Encryption | Required | From PKCS #1 |
| Subject. Common Name | See below | Recommended | |

### Signature algorithm

Use of md5WithRSAEncryption is recommended. The MD2 algorithm is curently supported, but support will be discontinued in some future release. In January 1996, RSA began recommending that vendors cease using MD2 due to a potential new weakness found in the algorithm.

**Subject Common Name for CA certificates**

Netscape recommends that the commonName for CA certificates be a user-readable name that describes the CA without the rest of the Distinguished Name. (Note the certificate should still contain a complete Distinguished Name.)

The Common Name will be displayed when the user chooses to view the list of trusted Certificate Authorities in the Security Preferences dialog box (reached from the Options menu). Examples include **Netscape Test CA** or **Certs-R-Us Level 42 CA**. Examples of names that are not recommended are **Certificate Authority** and **CA Root**.

### 4.6.4 Certificate Encoding

In Navigator 2.0, users (or administrators) can add new trusted Certificate Authorities to Navigator's certificate database. To add a new certificate, users point Navigator at a URL that contains the new CA certificate. Navigator will recognize and appropriately process a certificate encoded as follows:

**Encoding**

The certificate should be a binary DER encoded X.509 certificate with default 8-bit encoding.

**X.509 versions**

Navigator 2.0 can accept CA certificates that are X.509 version 1, 2, or 3. However, Navigator 2.0 ignores the fields issuerUniqueID, subjectUniqueID, and extensions.

**MIME type**

The certificate should be delivered to Navigator via the HTTP protocol, and should be identified by the newly defined MIME type **application/x-x509-ca-cert.** The body of the document should be the DER encoded certificate.

## CERTIFICATE SIGNING REQUESTS FOR SSL 2.0 CERTIFICATES

Certificate Signing Requests for SSL 2.0 certificates are issued via email.

## CERTIFICATE REQUESTS

Certificate Signing Requests are emailed to the certificate issuer. They take the following form:

Webmaster: webmaster@foo.com

Phone: 415-555-1212

Server: Netscape-Commerce/1.12

Common-name: www.foo.com

Email: webmaster@foo.com

Organization: FooBar Corp.

Org-unit: Web Content Division

Locality: Anytown

State: California

Country: US

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBOTCB5AIBADCBgDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlm
b3JuaWExEDAOBgNVBAcTB0FueXRvd24xFTATBgNVBAoTDEZvb0JhciBDb3JwLj
EdMBsGA1UECxMUV2ViIENvbnRlbnQgRGl2aXNpb24xFDASBgNVBAMTC3d3dy5
```

```
mb28uY29tMFowDQYJKoZIhvcNAQEBBQADSQAwRgJBANwLUqDA13nb1rGDSN
Nhl6HW77PZJrzec+I3gO8bYmcSTD8TLZ2u6eHaBsnR4qOcl+/7EoENhowKieTDv+xT
z8ECAQOgADANBgkqhkiG9w0BAQQFAANBANsX9Y9wYVLEnAZD0AaTnCzg0ek
A/9MnxCpfDml5SaNjOV2PxEXStjrijdP/Rb/1vYujpWBLaLS+e2IZwzvPpKI=
-----END NEW CERTIFICATE REQUEST-----
```

The actual certificate request is a DER-encoded PKCS #10 certificate request that is base64-encoded for email transport.

### 4.6.5 Certificate Responses

The Certificate Authority emails the signed certificate to the requester. The certificate is a DER-encoded X.509 version 1 certificate that is base64-encoded for email transport.

The server administrator saves the certificate to a file and points Commerce Server to the location of the certificate, using administrative utilities.

Here is a sample certificate:

This certificate will expire in 1 days

```
-----BEGIN CERTIFICATE-----
MIIB8jCCAVsCAgNNMA0GCSqGSIb3DQEBBAUAMEcxCzAJBgNVBAYTAlVTM
RAwDgYDVQQLEwdUZXN0IENBMSYwJAYDVQQKEx1OZXRzY2FwZSBDb21td
W5pY2F0aW9ucyBDb3JwLjAeFw05NTEyMTkxMDU4NTNaFw05NTEyMjAxMDU4
NTNaMIGAMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTE
```

QMA4GA1UEBxMHQW55dG93bjEVMBMGA1UEChMMRm9vQmFyIENvcnAuMR0
wGwYDVQQLExRXZWIgQ29udGVudCBEaXZpc2lvbjEUMBIGA1UEAxMLd3d3Lm
Zvby5jb20wWjANBgkqhkiG9w0BAQEFAANJADBGAkEA3AtSoMDXedvWsYNI02
GXodbvs9kmvN5z4jeA7xtiZxJMPxMtna7p4doGydHio5yX7/sSgQ2GjAqJ5MO/7FPPw
QIBAzANBgkqhkiG9w0BAQQFAAOBgQBmnCciKst05XSa7jbIWZ5b7/7eBGmNxlXy
JhPrVN+8OKGOL70XifXcangTmeuQ8MhVoUPJbZjkGmo6K/a3j1GTv1lHkjzAzUSh7
X7Y5kotfrj8OZxfsw+95qzGlPWE7f4Uv6RlV/fkXNygk0FemXUd5iPnkQ8kU66E2EJxy
BmMUQ==
-----END CERTIFICATE-----

## 4.7 Security in case of E-Commerce

Phil Gibson, National Semiconductor's director of interactive marketing, says such things can happen all too easily. "We have been touched by hackers ... in one case they were able to flip our front page for two minutes but we were able to detect and correct it without much trouble," he says.

The hackers were apparently just mischief makers, and National Semiconductor was ready for them. But if the company hadn't been set up to detect security breaches, the incident might have been much more damaging.

Virtual graffiti can tarnish your e-commerce image; hackers can go much further given the opportunity. There are endless reports of theft of credit card data and fraudulent funds transfers, which, if made public, can strike a tremendous blow to customer confidence. And industrial espionage poses an even bigger threat to your business.

Serious intruders are hard to catch, and unless you've got a good e-commerce security plan, you might not even know they've visited your site. So, while you've got communications to your server secured with Secure Sockets Layer and the server itself housed in a firewall defended extranet, what else can you do to protect your business?

Paul Hoffman, director of sales and marketing for the Hosting and E-Commerce Group of MCI Advanced Networks in Columbus, says, "Security is achieved by choosing the right technologies as you [build your e-commerce solution], which requires that you look at the data flows and their value so you know at what point you need to add extra security."

### 4.7.1 Overview of security approach in E-commerce

There are five main security issues to consider: Physical access to the e-commerce system during which data might be stolen or corrupted, malignant software which could deny or reduce service, network security breaches where users running personal Web servers on PCs could expose data, directed attacks against known problems with operating systems and applications, and protocol attacks where weaknesses in protocols are exploited.

The basic rules of general network security are fundamental to any practical e-commerce security plan. In fact, the only real difference is that your e-commerce platform is easily identifiable as a target. On a regular network, it's usually hard for a miscreant to figure out where the money is without a lot of work.

First, limit access. The fewer people who can get physical and administrative access to server systems, the better your security will be. Second, use available security tools and, third, perform regular audits to verify configuration and expected usage patterns.

Scheduled inspections are extremely important, as their purpose is to ensure that everything is working correctly, including your intrusion detection systems. This is an area where it pays to be extra cautious. Mike Dunn, chief technology officer for Dell Online, says, "We're incredibly paranoid ... we do continuous internal and external audits and we're always looking for problems."

The fourth rule is to protect complex systems with simple ones. A full-blown e-commerce server is very complex while a firewall is relatively less so. Protecting the former with the latter makes sense. And fifth, make backups and have a disaster recovery plan.

To explore e-commerce security issues, let's look at a scenario involving a basic e-commerce system. A supplier of office consumables wants to provide its larger customers with a corporate purchasing system. The system allows the customer to designate department managers, set spending limits and receive purchase reports.

Here are the challenges: how does the supplier the secure the transactions, authenticate the managers, and prevent hackers from getting in?

### 4.7.2 Securing the server

The first step is to create an extranet. Whether you're building your own site or outsourcing, there's no way to defend an e-commerce server without controlling the communications to and from it. A secure extranet houses the e-commerce server behind a firewall, which isolates the internal network from the outside world and explicitly allows specific protocol exchanges between customers and your e-commerce services.

For example, you might designate Hypertext Transfer Protocol (HTTP) and Secure Sockets Layer (SSL) as the only protocols your e-commerce system will use. In this case, you would specifically block all other protocols and be notified via alarm if someone attempts an unauthorized protocol exchange. This service is a function of many firewalls.

All commercial grade Web servers support basic authentication to ensure that users are who they say they are. Combine that with SSL implementation and you have a sound security foundation.

If you keep all software up to date with upgrades and patches, the rest of security comes down to the applications software and how you allow customers to interact with the e-commerce system.

Sonnet Financial, an international funds exchange business in San Mateo, Calif., processes millions of dollars of transactions every day through its e-commerce site. The company relies on a firewall and basic authentication over SSL. "We're not seeing a lot of hacker issues, but we've also done external security audits to make sure we're safe," says Ann Brighouse, director of product marketing. "Our clients are comfortable [with our security provisions]."

But what if you need even more security or you're simply more paranoid than most people. Say you're a supplier specializing in die castings for manufacturers. A hacker placing a bogus order could cost you thousands of dollars while unauthorized access of your firm's design documents lets your trade secrets out of the bag and compromises your competitiveness.

In this case, more robust security would be required. At the very least, you'd want to use SSL version 3, which supports digital certificate-based authentication for the client and server. You could use a third-party certificate authority such as Verisign or else set up your own private certification service. Digital certificates let users digitally sign electronic messages and files.

For even more sensitive scenarios, you could use a hardware token such as Security Dynamics' SecureID card, which generates a code and requires a user password. And if you need even more advanced security, consider using a biometric security system like fingerprint, voiceprint or retinal scans. The downside to biometrics is that the technology is relatively new and often requires custom implementations.

Digital certificates cost thousands of dollars at the server end and range from tens to hundreds of dollars for the client. Hardware tokens cost about $10 to $50 depending on configuration and volume, while server-based token authentication software costs about $5,000. Biometric devices such as retinal scanners are still very expensive, but fingerprint readers are rapidly becoming more affordable. For example, American Biometric's BioMouse costs roughly $250 per user.

In general, your company will foot the bill for its server-based e-commerce security systems. You could require customers to pay for the client end of the system if they want to do business with you, but it might be smarter to cover these costs yourself for your most valuable customers. This shows them that you're protecting their interests and it gives you more control over what they do on your e-commerce system.

## 4.8 The final approach

In spite of the array of security technologies available, you'll find the best security on systems that are well organized, well documented and well managed. Knowing what your e-commerce system is supposed to do and using appropriate technologies will prepare your site for safe transactions. The Boy Scouts wouldn't expect anything less.

# Chapter 5. Multilingual Approach to E-Commerce site

## 5.1 Concept of Multilingualism

**Your business depends on communicating with people around the world.**

Business communication has changed forever with the Internet, Intranets, e-mail, and other network-based communication systems. With information crossing the globe as never before, effective processing of foreign-language material is more important than ever to success in the global market. Your business must have access to extremely rapid, readily available, multilingual translation capabilities. Traditional human translation is often the preferred method for elegance and accuracy, but it is often too expensive and time-consuming to fulfill many of the new demands for multilingual communications.

Communication across language barriers is essential to the success of corporations expanding into foreign markets. Today the demand for translation services is greater than ever before. The ability to successfully translate from one language to another requires that human translators possess a high degree of skill in the areas of language comprehension, recognition and memory for at least two languages. Human translators use a variety of thought processes and skills to interpret the meaning of a sentence and communicate the meaning of that sentence in a different language. They are experts at the proper usage of language resources, such as term, phrase and grammar dictionaries to create a translation that will be clearly understood in the reader's target language. As a result, the automation of this human process has proven to be challenging and costly, and to date the publication of translated documents often requires the involvement of a human translator.

## 5.2 Challenges and Future Development of Multilingual Technology

Currently, the challenges which technologists face are problems related to machine translation, conceptual structuring of multilingual Web pages, conceptual indexing in multiple languages, standards for character encoding, multilingual browsers and the operations with Web technology (e.g. HTML, HTTP and the Internet). Unicode Standards, so far, have solved many character encoding problems in diverse languages and have ensured display of characters without relying on meta data. Yet huge demands for character storage for more languages, especially Chinese characters, bring a big problem as more bits in character encoding are necessary. This will affect data transmission rates (Peters and Picchi, 1997).

For character display, many software companies put great effort into developing multilingual browsers, which enable users to view different languages on the Web. Although these localized applications can satisfy many non-English speaking users' needs, they are not internationalized applications for display and use in word processors. A universal browser or an adaptable browser, which consists of internationalized and localized elements, can solve the problem. If a new script is found in the text, it can be upgraded on the fly.

At present, machine translation is far from producing quality translation work. In addition, machine translation is quite important for search retrieval. Technologists should focus more on studying string-based retrieval (e.g. different word forms), lexical semantics and dictionaries or thesaurus based translations. This will result in better retrieval of relevant results by using multilingual search engines.

Since the trend of sharing localized information (e.g. multilingual documents) is becoming more and more common, in my opinion, the future development of multilingual technology will focus on improving information retrieval in diverse languages as well as finding solutions to current problems. In addition, struggling between producing localized or internationlized applications will be continued. The demands for viewing multiple languages on the Web will be an essential force driving the evolution of multilingual technology.

## 5.3 Multilingual solution

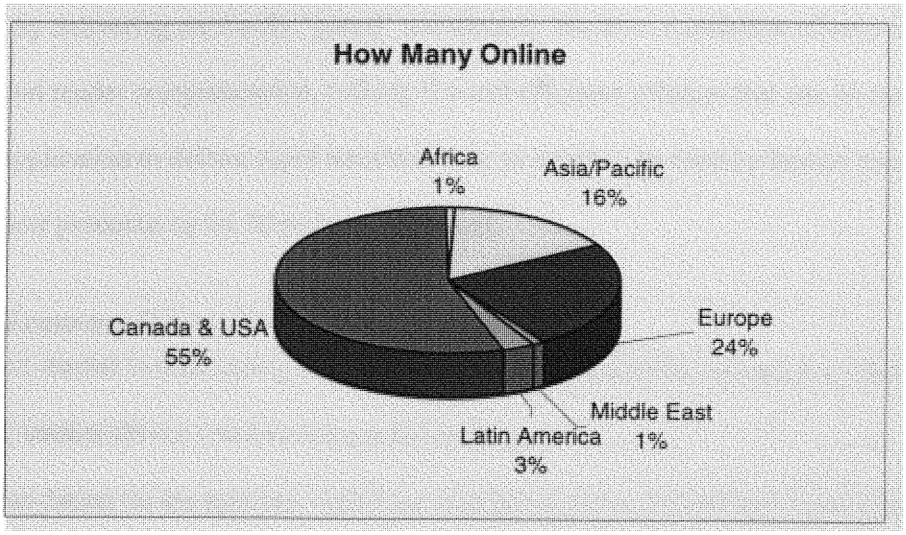
### 5.3.1 Machine Translation

Computerized translation (or "machine translation") is a highly cost-effective way to meet the demands for multilingual Web content, e-mail, or other text-based communications. This complex technology translates texts from one human language to another. Translator at the heart of the Translation Server interprets the structure of sentences in the source language and generates a translation based on the rules of the target language. [22]

### 5.3.2 What the Translation Server can do for you

The Translation Server enables network users to produce extremely rapid draft-quality translations. Your employees and customers will gain instant access to foreign-language content. The Translation Server delivers substantial gains in productivity and efficiency that would be impossible otherwise.

Over the ages, technology has been dedicated to overcoming obstacles, whether it be the construction of great bridges to span rivers, the building of reliable ships to cross oceans, or the development of printing presses and, much later, the telephone to allow the immediate dissemination of ideas. As in the case of many great technological breakthroughs, the Internet—a tool that provides up-to-the-minute news and information at the fingertips of every person around the globe—overcomes one obstacle only to magnify another. The Internet, while available on a global level, underscores the serious limitations in our ability to communicate across language barriers. Today, only 53.76% of all Internet users speak English and in 2005 less than 43% will speak English.



**5.1 How many Online? [11]**

In the next 6 years, the Internet will experience a 150% increase in usage among non-English speakers with the majority of new users from Asian/Pacific and Latin American countries. Clearly, the power of the Internet is only as great as our ability to communicate across it.

While human translation is unquestionably the preferred method for producing accurate and localized translations, it remains prohibitively expensive and too time consuming to meet the new demands of businesses and individuals working at Internet speeds. Today, multinational corporations are communicating with their international offices and partners on a daily basis. In order for organizations to continue to maintain a competitive edge, personnel must have the ability to collaborate with colleagues around the globe. Successful partnerships with international colleagues require that personnel have access to immediate translations of multilingual communications via workgroups and e-mail as well foreign documents and intranets.

The emerging global connectivity via the Internet, intranets and other networks has created an urgent need for inter-language communication tools that provide immediate "gisted" translations. "Gisted" translations are draft-quality translations that provide individuals and professionals with the meaning of the original foreign-language document to determine the relevance to themselves or their business. Machine translation—that is, translation done by computer—responds to this new demand by delivering on-the-fly "gisted" translations. Machine translation offers a high level of accuracy and reader comprehension, making it a cost-effective solution that can be used as a stand-alone application to deliver rapid translations or as a tool to be used by human translators (increasing their productivity by 30 percent and more).

### 5.4 Global Economy Drives Translation Market Trends

The translation market is undergoing a rapid evolution characterized by several key trends that sophisticated, market-driven vendors can capitalize upon.

Consumer Translation on the Internet—Machine translation is fast becoming a communication-enabling technology for the Internet and corporate intranets. The Internet's massive flow of polyglot digital information requires "on-the-fly" translation capabilities so that parties can communicate effectively.

Increased Consumer Need—The rapid growth of the Internet has led to an increased consumer use of translation.

Internet Translation Services—Internet service providers will begin to offer online access to machine translation services as the Internet promotes seamless global communication.

Strategic Alliances—Strategic alliances between vendors of machine translation tools and translation workbenches will develop as key synergies are realized.

Digital communication is expected to create an explosion in the demand for automatic translation software as cross-language e-mail, cross-language chat, and multi-language forums become standard methods of communication.

Machine translation vendors will use their products to provide services to casual users and users who have low-volume, ad-hoc translation requirements.

Enterprise Products—Machine translation systems will quickly migrate from single user, PC-based products to networked products.

The demand for products which offer network compatibility is increasing, with more and more companies choosing to implement products which can be used on local and wide area networks.

The networking trend will result in full-scale translation management systems that are fully integrated with document management infrastructures.

The technologies that support the larger document environment are moving towards workgroup configurations that manage document resources in a more systematic way.

Translation tools which are appropriately configured for workgroups, incorporating on-site and remote workers, and capable of being networked among different workgroup sites, will be the most viable of the translation software products.

Translation Portals—Translation software is available over the Internet to service both individual and business users.

Software providers are increasingly migrating to the application service provider (ASP) distribution model of one-to-one software leasing. ASPs create new markets from resource-constrained organizations that might not be able to afford enterprise translation software.

End users benefit from access to best-of-breed solutions without paying for costly upgrades and IT staff for in-house systems.

Reduced Cost of Translation—As a result of market growth, automatic translation will be affordable in relation to the value that it delivers, as the need for cross-language communication becomes increasingly pervasive.

## 5.5 Powering Global Communications

Today, the global economy is quick to feel the effects of world events due to the velocity at which information and news is received across the Internet. Businesses and individuals need to understand and have the ability to quickly respond to worldwide changes and events. However, if those changes and events are communicated in a foreign language, an instantaneous, "gisted" translation may be the only solution to overcoming a language barrier and responding appropriately. Despite limitations, machine translation systems will become an important and indispensable tool for businesses and individuals where global communication is a priority.

Machine translation offers users two application directions. The first is the assimilation of translated foreign-language information for one's own purposes and the second is the dissemination of translated native-language information for receipt by a foreign language individual. Assimilation and dissemination each carry their own unique demands and requirements for quality, speed, flexibility and power.

Assimilation

Machine translation systems deliver significant power to users as they assimilate or receive information. Growth of the Internet and global research, as well as the increase in e-mail, corporate intranets, workgroup communication systems, multilingual user groups, and document management systems have created demand for solutions that allow users access to translations that give them the "gist" of the message, web page or document. Ideal for people who need instantaneous access to translations, gisting solutions allow users to quickly determine the relevance and meaning of various content to their business or interests.

### Dissemination

Many businesses and organizations need to disseminate or distribute translated documents that must be concise and as understandable as if written by a native of the target language. This requires the ability to localize language that today only professional translators can offer. Machine translation, however, is a cost-effective way to provide professional translators, writers and editors with a tool that improves the productivity of their work groups. Machine translation produces extremely quick but imperfect translations that require post-editing. Despite these post-editing requirements, productivity gains of 30 percent or more are possible using programs like the *Enterprise Translation Server*™ by Transparent Language as part of the translation process

## 5.6 What is Machine Translation?

Machine translation systems (MT systems) are linguistically sophisticated translation technology products programmed with comprehensive dictionaries and a collection of linguistic rules that translate one language into another without relying on human translators. [23] An MT system interprets the structure of sentences in the source language (the language the user is translating from) and generates a translation based on the rules of the target language (the language the user is translating to). The process involves breaking down complex and varying sentence structures, identifying parts of speech, resolving ambiguities, and synthesizing the information into the components and structure of the new language.

There are three basic processing methods for computer-aided translations:

Direct This simple method translates word by word without interpreting sentence structure. The result is a translation that is in the word order of the source text, which can result in a significant loss of meaning and readability.

Benefits Numerous language pairs available due to short development time per language.

Drawbacks Comprehension and translation quality is often unacceptable.

Transfer Used by general translation engine,, this method performs semantic analysis of the source language sentences and then transfers that information into the target language based on a set of rules specific to that language direction. The quality of the resulting translations is significantly higher than the simple Direct method translations.

Benefits Translation quality is superior to Direct method.

Drawbacks Development of language pairs is time consuming and expensive.

Interlingua In theory, this method would input the source language into an intermediate repository where expressions, sentence semantics and forms of expression would be replaced, independent of any language, and then the intermediate language would be translated into the target language. This theoretical method has yet to be used with any commercial applications.

Benefits The promise of high quality translations and rapid development of language pairs.

Drawbacks No commercially available application on the market.

The Basic Process of Transfer Method Machine Translation Systems Used by various search engine is

- Segmenting—The source document is divided into paragraphs, then sentences and finally words, all the while retaining formatting information. A sequence of filtering and scripting operations makes this process very flexible within the system.

- Morphological analysis—The individual words are looked up in the dictionaries and phrases are identified. *Translator* has the ability to recognize a word in various forms; for example, identifying that "talking" is the gerund form of "talk."

- Functional analysis—*Translator* determines how each word is functioning in the sentence and determines the part of speech for words that can function as more than one part of speech. *Translator* also determines which words are functioning as a phrase.

- Syntactic analysis— *Translator* determines the grammatical structure of each sentence, aided by information about the meaning of the words in the sentence.

- Transfer—The elements of the sentence are reordered, inserted or deleted to form the syntax of the new language.

- Generation—Creating the final sentence in the new language is a multi-step process that, in effect, reverses the steps for analyzing the source sentence. When the process is complete, *Translator* restores the original formatting information as it applies to the new text.

In addition to the translation process, there are a series of dictionary authoring tools associated with *Translator*. The dictionary authoring tools are included with high-end versions of Transparent Language translation products to enable users to control and enhance translation by customizing the dictionary content. The linguistic tools are aimed at tuning language analysis rules and are not intended for end users of the products, but by linguists either creating a new language pair or enhancing the rules for an existing pair.

## 5.7 Translator Architecture

The Translation Server uses Transparent Language's Translator to translate text from one human language into another.

### 5.7.1 Components

Translator can be broken down into three major components: filtering and formatting elements, dictionaries, and language rules.

- **Filtering and Formatting**

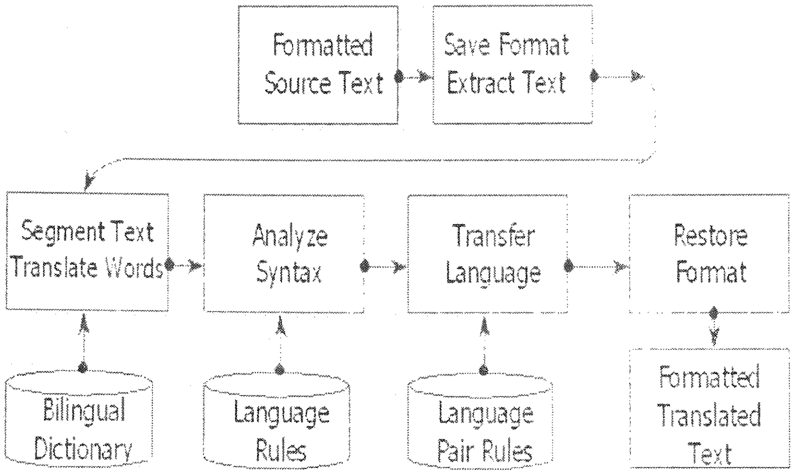
  Translator sophisticated filtering system allows the Translation Server to distinguish between formatting code and translatable human language. After the translation is complete, the formatting of the source text is re-applied to the translated text, thus preserving the look of the original document.

- **Bilingual Dictionaries**

  Dictionaries are the lexical backbone of Translator. They contain the bulk of the raw information by which text is translated. Each dictionary entry contains detailed grammatical and syntactical information about both the source word and the target word. This information allows Translator to identify exactly how words are used in a sentence and to replace that word with a grammatically and syntactically accurate foreign-language equivalent.

- **Language Rules**

  Language rules specific to the source and target languages are invoked to analyze and later to generate sentences. Language analysis rules allow Translator to parse, or break down, a sentence into its components. Language synthesis rules contain language-specific algorithms for forming specific structures, such as compound verbs, negation, questions, imperatives, and placement of adverbs and adjectives.



**5.2 Language Transfer methodology [23]**

### 5.7.2 Methodology

Translator uses the transfer method for computer-aided translations. Translator produces a translation in five steps.[24]

**1. Save Format / Extract Text**

A sequence of filtering and scripting operations allow Translator to distinguish between formatting code and translatable text. The formatting code is saved for later re-application to the translation.

**2. Segmenting and Word Identification**

The translatable text is then divided into paragraphs, sentences, and finally words. Individual words are looked up in the dictionaries, and phrases are identified.

**3. Analyze Syntax**

Translator determines the function of each word in the sentence.

**4. Transfer Language**

Translator determines the grammatical structure of each sentence, aided by information about the meaning of the words in the sentence. Elements of the sentence are reordered, inserted, or deleted to form the syntax of the target language, in effect reversing the steps for analyzing the source sentence.

**5. Restore Format**

When the translation is complete, Translator applies the formatting code from the source document to the translated text.

## 5.8 General Methodogy to translate in different languages

### 5.8.1 Overview

The general framework that some companies utilizes in all its Machine Translation (MT) systems is proven to be powerful and effective. In its long history, many improvements have been made to the original design, resulting in great modularity.

Use of existing modules, as well as consistent use of similar methods across different languages, when applicable, will allow quick and efficient development of a functional prototype system for any new language pair.

Their architecture is also very flexible and allows introduction of innovative methods. In fact, with every new language added to the there inventory some new techniques have been tried in response to new challenges of that language. Often such innovations are later found to be also applicable to other language pair systems.

### 5.8.2 Methodology

Translator Methodology is a sentence-by-sentence approach, concentrating on individual words and their dictionary data, then on the parse of the sentence unit, followed by the translation of the parsed sentence.

- **Modularity**

Three major groups describe the Translator architecture: Dictionary, Systems Software and Linguistic Software. Each of these consists of a great number of modules which all work together to create a fully automatic MT system.

- **Dictionary**

Translator traditionally employs three distinct, but interconnected types of dictionaries for the MT systems of all languages.

1. **Stem Dictionary.** The basic dictionary is a single-word "Stem Dictionary". Words are entered in a basic form with codes to indicate inflectional patters, part-of-speech, syntactic behavior, semantic properties, and target language meanings together with codes needed for the target word generation. Homographic forms with part-of-speech ambiguity are entered separately for each part-of-speech, cross-referenced to the basic entries and indexed by type of part-of-speech ambiguity. The source language related portion of the Stem dictionary is complemented by transfer and target information for each word into several target languages.
2. **Expression Dictionary**. This is the dictionary of multiple-word expressions. These expressions include co-occurrence-based and rule-based expressions, and may range from simple noun phrases, to expressions containing translation rules based on the syntactic or semantic link between individual words, or entire classes of words. Words in the Expression dictionary are given in their "basic" form, and indexing to the Stem Dictionary allows execution of the rule for all inflected forms or alternate spellings as recognized in the Stem dictionary.
3. **Customer Specific Dictionary (CSD).** A PC/Windows based CSD allows the user to enter terms (words and a set of pre-defined types of expressions) which were not found in the main dictionaries. The user may also globally or conditionally change

meanings found in the main dictionaries. The CSD is designed for the individual or industrial user with limited needs.

### 5.8.3 System Software

A body of systems software, consistent across the various SYSTRAN language pairs, handles formatting, character conversion, user interface, sentence and word boundary determination, dictionary and morphology lookup, and not-found word treatment. It controls the flow of linguistic modules and creates final formatted output. Also supported are a variety of tools for dictionary preparation, quality assurance, corpus manipulation, and parsing diagnostics

#### 5.8.3.1 Linguistic Software

**PARSER**. The most challenging aspect of any MT system is the parser, the module that analyzes each sentence and attempts to build up representations of the source sentences [23]. Translator parses with a battery of procedural modules which resolve, step by step, various syntactic and semantic relationships and assign structure within the sentence. The Translator parser is deterministic in nature, so each module makes firm decisions and passes the results on to the next module. The advantage is that every sentence, even an incomplete or malformed one, will be parsed and therefore translated. The disadvantage of such determinism is that incorrect decisions may be passed on and compounded from module to module. Translator is able to soften this by several mechanisms that flag uncertain decisions. Translator's final step in this checking process is a Filter program, which identifies the major parse errors.

**Target Language Translation Modules**. After a parse of the input sentence has been constructed, algorithms for the construction of a translation are invoked. Translation information, on both the word and expression levels, is derived during dictionary lookup and the parsing phases of the translation, for use by two distinct Transfer and Synthesis modules. The Transfer component performs situation-specific restructuring, depending on the degree of difference between source and target languages. It is the only module, besides the dictionary, which relates to both source and target language, and it is rather small when the two languages are closely related.

**Synthesis Module.** Following this, the Synthesis module generates the target language strings, which correspond to the information provided by all previous modules. Synthesis is a source-language independent module. The Synthesis modules contain sophisticated algorithms for creating specialized target language constructs, such as negation, questions, verbs with complete morphology, placement of adverbs, and articles etc.

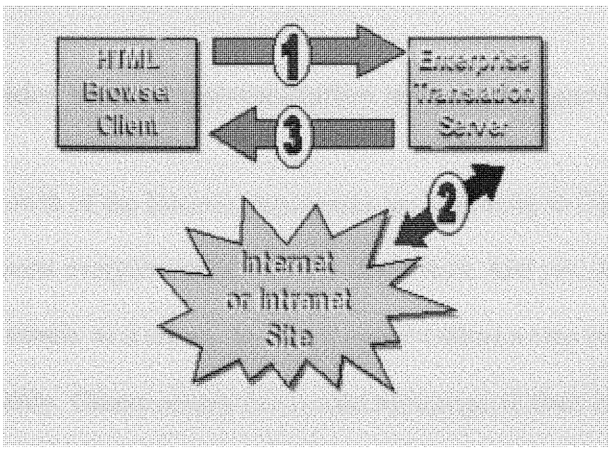
## 5.9 Translation of Web Pages

The translation Server can translate web pages in real time. Access to an HTML Client for web pages allows network users with Netscape Navigator 3.0 (or higher) or MS Explorer 3.01 (or higher) to request the translation of any web page available to the server.

This translation interface is delivered to the customer as an HTM file that has to be modified by the System Administrator to reflect the network installation of the Translation Server . [25]

The HTM file is then integrated into the business's Intranet or Internet site as a Web page, where it can be used by network users with access to that part of the network.

### 5.9.1 How it works



5.3 web page architecture for translator [25]

With the HTML Client for Text, the end user pastes a URL into the appropriate dialog field. The user indicates the desired language pair in the drop-down menu and then clicks on the TRANSLATE button.

The Server processes the request and delivers a dynamically generated web page to the end user. The end user receives a translation that preserves the illustrations and formatting of the original web page.

# Chapter 6. Implementation

## 6.1 Points to be consider before Implementation of the site regarding E-commerce .

With the astonishing growth of the Internet, businesses are beginning to find new ways to expand their opportunities. It seems everyone has a web site these days. And yet, the task of setting up a web site is often not as simple as it seems. In fact, I would venture to say that most business sites lack focus and functionality. Others simply fail to take advantage of their full potential.

The Internet is proving to be the great equalizer, allowing the smallest of businesses to access markets and present a presence that allows them to compete against the giants in the industry. So exactly how does a small business compete?

Given the numerous questions we field everyday and the many options available to businesses, I thought it would be beneficial to lay out a brief outline of how a business should go about establishing an on-line presence.

### 6.1.1 Do you need a web site?

This should be the first question asked. A business should think about what they intend to accomplish by establishing a web site. Once answered, this will also guide you through some of the options available.

There are three main reasons why businesses establish web sites:

- Marketing
- Customer Support
- Sales

Most current sites on the web are merely a marketing presence and this may be your only goal. Determining the purpose of your site will set a framework for your design.

Many companies have found that the Internet is a wonderful resource to offer customer service, provide product specifications and furnish on-line answers to the numerous questions they receive and deal with every day. If this goal is also part of your web site, then you have to make it easy for your customers to find the information they are after.

Many sites are setup to go beyond general marketing and to actually generate an order, often unassisted by any human interface. The simplest version of this might include instructions to print a page, fill in order details and fax it to a given number. More sophisticated sites have an easy to maneuver ordering process with proper order calculations done including shipping and sales tax. The most advanced sites allow an option of accepting and approving the credit card information while the customer is on-line.

### 6.1.2 Budget

Setting up and running a business web site will cost money. Having determined your reasons for creating your site, you should be better able to consider the costs. The difficulty here is that the costs can vary substantially. This is new technology, with numerous options available. It would behoove a business owner to do a little research in each area where dollars are to be spent.

The main questions to ask in starting this process are:

Will I own/run my own server? Do I need to?

How will my site/server be connected to the Internet?

Who will design my site?

Who will maintain my site, and how extensive of a process is this?

Do I want to accept orders on-line?

Will I need to or want to interface my web page with existing databases, order systems or accounting systems.

With these simple questions, you can see how vast your options are. Some companies have spent millions "developing" their web sites and yet many others have put up a substantial site for next to nothing.

In this article, I have assumed that you are a small business wanting to "get your feet wet" with a site and keep your expenditures to a minimum.

### 6.1.3 Setup and Design

There is no shortage of experts who will help you design and put up a site. Site size and complexity can vary immensely. Many computer literate individuals have chosen not to go to consultants at all. With the excellent web design development tools available today, such as Microsoft FrontPage, many are able to get a web site designed with only a few days work. If you do the work yourself, check it on both Netscape and Microsoft browsers and design for a 15" monitor. Also, avoid the temptation to over design. Adding large graphics, animation and music may be impressive to the designer, but most users don't have the plug ins to hear the sound and won't wait for your fancy graphics to load on their 28,800 (or worse) Internet connection.

Consider establishing your own domain name if you are serious about your site. You can apply directly to InterNIC (http://www.internic.net) to get an address such as www."your_company".com which will be perceived as more credible than an obviously hosted site. The fee to InterNIC ($70 for two years) is well worth it.

Of course you will have to find an ISP (Internet Service Provider), usually local, and make arrangements to either host your site or server or provide appropriate connections. Call and discuss the options and then shop around.

### 6.1.4 Attracting Customers

There is an endless stream of information available on the Internet about how best to market your site. Suffice it to say that registering your site with a few search engines is the minimum. Because this information is so plentiful, I intentionally skip over it here. However, it should be noted that the net is an ever-changing environment and marketing should be considered more than a one time effort at the time you create your site.

- **Moving from Marketing to Selling**

So you have your web site up and your products listed, if not pictured. Your phone number is available so viewers can call and order your product. If you've done your job well, some will call and you can start generating orders. But why not make it easier than that? Why not allow your customer the additional option of ordering directly on-line with a credit card while he or she is viewing your site? Here's what you need to consider.

**You need a "merchant account"**

Merchant Account is an industry term meaning a banking relationship which allows a business to accept credit cards. Most existing businesses will already have established such a relationship and you certainly need this capability to accept credit card orders on the net. This goes without saying, but many small businesses have not yet established the banking relationships necessary to accept credit cards. This is really a first step. There are many consultants advertising on the web who can assist a business, even a new startup, to get setup for accepting credit cards. You may or may not need to buy processing software or hardware depending on how you plan to clear your transactions. The cost for setting up an account varies but can easily run to $300 or more.

**To accept credit card orders on the net, you will need a "secure server"**

There is a lot of concern about security on the net. Most of this concern is due to misinformation and the Internet continues to prove itself as a safe medium for transactions. It is important to follow established conventions in Internet security however, which means utilizing a secure server for credit card transactions.

A secure server is one running software capable of establishing a "secure" connection with your customer's Internet browser using SSL (secure socket layers) technology which encrypts all transmitted information. Most net buyers insist on this connection before entering credit card information. You can usually find a secure server to host your site. You don't need a secure server if you outsource your order processing as discussed below.

**You will need an order form**

This sounds simple enough. However this can be a very complicated piece of software. You have to be able to present all your products, prices and options (sizes, colors etc.). Before you can request credit card information you need to be able to automatically subtotal the order, add shipping and handling and calculate sales tax if appropriate, based on the buyer's location. Writing this capability into your web pages requires a lot more than some HTML knowledge. You can purchase software to do this and try and integrate it in to your site, or you can outsource this function by subscribing to a service such as Anacom's.

**On-line clearing**

You also have the option of considering clearing (or authorization) of the credit card, while your customer is on-line. This feature may be imperative if you are delivering information or allowing a download of purchased software from your site. Even if you are shipping a product after the fact, this may prove to be a great convenience to you. If your business is solely Internet based, this option would allow you to avoid the expense of purchasing processing equipment or software which can be quite expensive. Unfortunately, designing on-line clearing capability is extremely complex and thus, this option is best undertaken through an outsourcing solution. Unlike general web site design, there are not many consultants available with expertise in this area.

**Accounting**

You need a methodology of tracking your orders. These can include, email notification, electronic receipts, on-line reports, internal database tracking, on-line query search capability, conversion programs, etc. It is easy to go overboard on some of these things and a lot of money can be spent trying to integrate online ordering with existing business functions. We always recommend that businesses starting on the web not try to be too sophisticated in this area up front. If you get your orders and have a paper trail as a minimum, you can always upgrade in this area later. If you use an outside service, you may have a lot of backup information available to you to help.

### 6.1.5 Technical Challenges

A simple web site thus may not be so simple if it is to be effective. A functional site contemplating online ordering requires expertise in four different areas.

HTML (hypertext markup language - standard for the Internet) basic page design

CGI scripting (or programming equivalent) for order form functionality

ODBC (Open database connectivity) interface commands for data tracking

Special programs for online clearing option

If any part of this puzzle is not available to you in-house, there is a world of consultants. The other alternative is outsourcing.

Outsourcing - a cost effective alternative

Outsourcing is the utilization of a third party service company to provide you with those pieces of the puzzle that complete the total functionality of the business process. In E-Commerce, the most cost effective way to meet your goals is often to outsource that portion of your needs that you don't have the expertise for in-house. This can allow you to get up and running much faster and concentrate on your business rather than getting mired down in technical matters.

## 6.2 Resources for Thesis

Following resources I have used for my thesis

- HTML
- DHTML
- Just add Commerce
- Java
- Plug ins

### 6.2.1 HTML

HTML (Hypertext Markup Language) is the set of "markup" symbols or codes inserted in a file intended for display on a World Wide Web browser. The markup tells the Web browser how to display a Web page's words and images for the user. The individual markup codes are referred to as elements (but many people also refer to them as tags). HTML is a standard recommended by the World Wide Web Consortium (W3C) and adhered to by the major browsers, Microsoft's Internet Explorer and Netscape's Navigator, which also provide some additional non-standard codes. The current version of HTML is HTML 4. However, both Internet Explorer and Netscape implement some features differently and provide non-standard extensions. Web developers using the more advanced features of HTML 4 may have to design pages for both browsers and send out the appropriate version to a user. Significant features in HTML 4 are sometimes described in general as dynamic HTML. What is sometimes referred  as HTML 5 is an extensible form of HTML called XHTML. [26]

### 6.2.2 DHTML

Dynamic HTML is a collective term for a combination of new Hypertext Markup Language (HTML) tags and options, style sheets, and programming that will let you create Web pages more animated and more responsive to user interaction than previous versions of HTML. Much of dynamic HTML is specified in HTML 4.0. Simple examples of dynamic HTML pages would include (1) having the color of a text heading change when a user passes a mouse over it or (2) allowing a user to "drag and drop" an image to another place on a Web page. Dynamic HTML can allow Web documents to look and act like desktop applications or multimedia productions.

The features that constitute dynamic HTML are included in Netscape Communications' latest Web browser, Navigator 4.0 (part of Netscape's Communicator suite), and by Microsoft's browser, Internet Explorer 4.0. While both Netscape and Microsoft browsers support HTML 4.0, some additional capabilities are supported by only one of the browsers. The biggest obstacle to the use of dynamic HTML is that, since many users are still using older browsers, a Web site must create two versions of each site and serve the pages appropriate to each user's browser version.

The Concepts and Features in Dynamic HTML

Both Netscape and Microsoft support:

- An object-oriented view of a Web page and its elements
- Cascading style sheets and the layering of content
- Programming that can address all or most page elements
- Dynamic fonts

## An Object-Oriented View of Page Elements

Each page element (division or section, heading, paragraph, image, list, and so forth) is viewed as an "object." (Microsoft calls this the "Dynamic HTML Object Model." Netscape calls it the "HTML Object Model." W3C calls it the "Document Object Model.") For example, each heading on a page can be named, given attributes of text style and color, and addressed by name in a small progam or "script" included on the page. This heading or any other element on the page can be changed as the result of a specified event such a mouse passing over or being clicked or a time elapsing. Or an image can be moved from one place to another by "dragging and dropping" the image object with the mouse. (These event possibilities can be viewed as the reaction capabilities of the element or object.) Any change takes place immediately (since all variations of all elements or objects have been sent as part of the same page from the Web server that sent the page). Thus, variations can be thought of as different properties of the object.

Not only can element variations change text wording or color, but everything contained within a heading object can be replaced with new content that includes different or additional HTML as well as different text. Microsoft calls this the "Text Range technology."

## Style Sheets and Layering

A style sheet describes the default style characteristics (including the page layout and font type style and size for text elements such as headings and body text) of a document or a portion of a document. For Web pages, a style sheet also describes the default background color or image, hypertext link colors, and possibly the content of page. Style sheets help ensure consistency across all or a group of pages in a document or a Web site.

Dynamic HTML includes the capability to specify style sheets in a "cascading" fashion (that is, linking to or specifying different style sheets or style statements with predefined levels of precedence within the same or a set of related pages). As the result of user interaction, a new style sheet can be made applicable and result in a change of appearance of the Web page. You can have multiple layers of style sheet within a page, a style sheet within a style sheet within a style sheet. A new style sheet may only vary one element from the style sheet above it.

Layering is the use of alternate style sheets or other approaches to vary the content of a page by providing content layers that can overlay (and replace or superimpose on) existing content sections. Layers can be programmed to appear as part of a timed presentation or as the result of user interaction. In Internet Explorer 4.0, Microsoft implements layers through style sheets. Netscape supports the style sheet approach but also offers a new HTML <LAYER>...</LAYER> tag set (that Microsoft does not support). Both approaches are being considered by the W3C

Working Committee and both companies say they will support whatever W3C decides will be the recommended approach.

### Programming

Although JavaScript, Java applets, and ActiveX controls were present in previous levels of Web pages, dynamic HTML implies an increased amount of programming in Web pages since more elements of a page can be addressed by a program.

### Dynamic Fonts

Netscape includes dynamic fonts as part of dynamic HTML. This feature of Netscape's Navigator browser in its Communicator suite lets Web page designers include font files containing specific font styles, sizes, and colors as part of a Web page and to have the fonts downloaded with the page. That is, the font choice no longer is dependent on what the browser provides.[26]

### 6.2.3 Java

Java is a programming language expressly designed for use in the distributed environment of the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces a completely object-oriented view of programming. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. It can also be used to build small application modules or applets for use as part of a Web page. Applets make it possible for a Web page user to interact with the page.

The major characteristics of Java are:

The programs you create are portable in a network. Your program is compiled into Java bytecode that can be run anywhere in a network on a server or client that has a Java virtual machine. The Java virtual machine interprets the bytecode into code that will run on the real computer hardware. This means that individual computer platform differences such as instruction lengths can be recognized and accommodated locally just as the program is being executed. Platform-specific versions of your program are no longer needed.

The code is "robust," here meaning that, unlike programs written in C++ and perhaps some other languages, the Java objects can contain no references to data external to themselves or other known objects. This ensures that an instruction cannot contain the address of data storage in another application or in the operating system itself, either of which would cause the program and perhaps the operating system itself to terminate or "crash." The Java virtual machine makes a number of checks on each object to ensure integrity.

Java is object-oriented, which means that, among other characteristics, similar objects can take advantage of being part of the same class and inherit common code. Objects are thought of as "nouns" that a user might relate to rather than the traditional procedural "verbs." A method can be thought of as one of the object's capabilities or behaviors.

In addition to being executed at the client rather than the server, a Java applet has other characteristics designed to make it run fast.

Relative to C++, Java is easier to learn. (However, it is not a language you'll pick up in an evening!)

Java was introduced by Sun Microsystems in 1995 and instantly created a new sense of the interactive possibilities of the Web. Both of the major Web browsers include a Java virtual machine. Almost all major operating system developers (IBM, Microsoft, and others) have added Java compilers as part of their product offerings.

The Java virtual machine includes an optional just-in-time (JIT) compiler that dynamically compiles bytecode into executable code as an alternative to interpreting one bytecode instruction at a time. In many cases, the dynamic JIT compilation is faster than the virtual machine interpretation.

JavaScript should not be confused with Java. JavaScript, which originated at Netscape, is interpreted at a higher level, is easier to learn than Java, but lacks some of the portability of Java and the speed of bytecode. Because Java applets will run on almost any operating system without requiring recompilation and because Java has no operating system-unique extensions or variations, Java is generally regarded as the most strategic language in which to develop applications for the Web. (However, JavaScript can be useful for very small applications that run on the Web client or server.) [27]

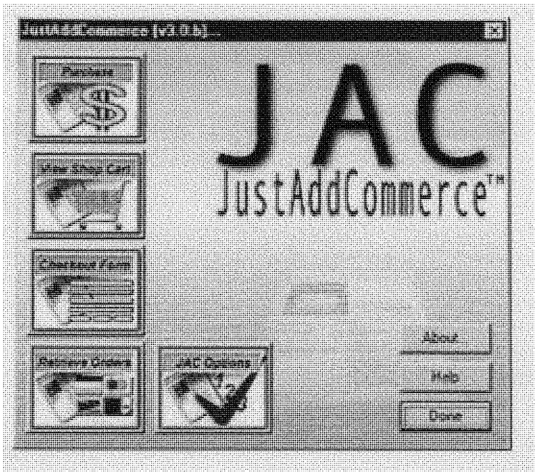
### 6.2.4 Just Add Commerce

- JustAddCommerce [28] is a professional shopping cart that can be quickly and easily added to any existing web site using Microsoft FrontPage's editor.

- JustAddCommerce has all the features your business will need to conduct electronic commerce on the Internet (credit card processing, tax calculations, shipping calculations, etc.).

- JustAddCommerce lets you build the site the way you want... No templates or generic web pages like those other shopping carts!

- JustAddCommerce is easy to use and requires no programming skills or knowledge of HTML.



**6.1 JAC window [28]**

Advantages of JAC

- 100% compatibility with ALL web servers

- Professional SSL CGI shopping cart technology written in C++ you use your own credit card merchant account .

- We are a true electronic commerce network and not an Internet Service Provider.

- JustAddCommerce software interfaces with the secured JustAddCommerce Transaction Network so you can be assured of compatibility, reliability and security.

Why trust other shopping cart programs that reside on a web builder's own servers when you can have the best technology in the business with no limitations.

- JustAddCommerce works with all browsers to guarantee that all your customers will be able to order from your web site. You are not excluding customers with older browsers and JustAddCommerce works with proprietary browsers like AOL, WebTV, Windows CE, etc.

- JustAddCommerce does not use any Java, or JavaScript... You can always be assured that all your customers viewing your web site will be able to order no matter what browser options they have set or disabled.

### 6.2.5 Plug-Ins

Even if someone is new to the Internet, someone has probably been hearing about multimedia on the Web — listening to audio, watching animations and videos, and even playing in three dimensional space. Life online can be a much richer experience when someone is not 7restricted to just words and pictures. Sound and movement make information come alive.

To experience multimedia online, someone should have a computer with a sound and video card. Then what one needs are special pieces of software called plug-ins. A plug-in extends the capabilities of your web browser, like Netscape Navigator, or Microsoft Explorer, turning your computer into a radio or television. Thus, plug-ins are software programs that extend capabilities of Netscape Navigator in a specific way giving you for example the ability to play radio samples or view video movies from within Navigator. Many plug-ins and controls can be downloaded for free from the Internet, some of are listed as follow:

## Plug-Ins by Category

MultiMedia: MultiMedia Plug-Ins, AVI, QuickTime, ShockWave.

Graphics: Graphic Plug-Ins, PNG, CMX, DWG.

Sound: Sound & MIDI Plug-Ins, MIDI, RealAudio, TrueSpeech.

Document: Document Viewer Plug-ins, Acrobat, Envoy, MS word.

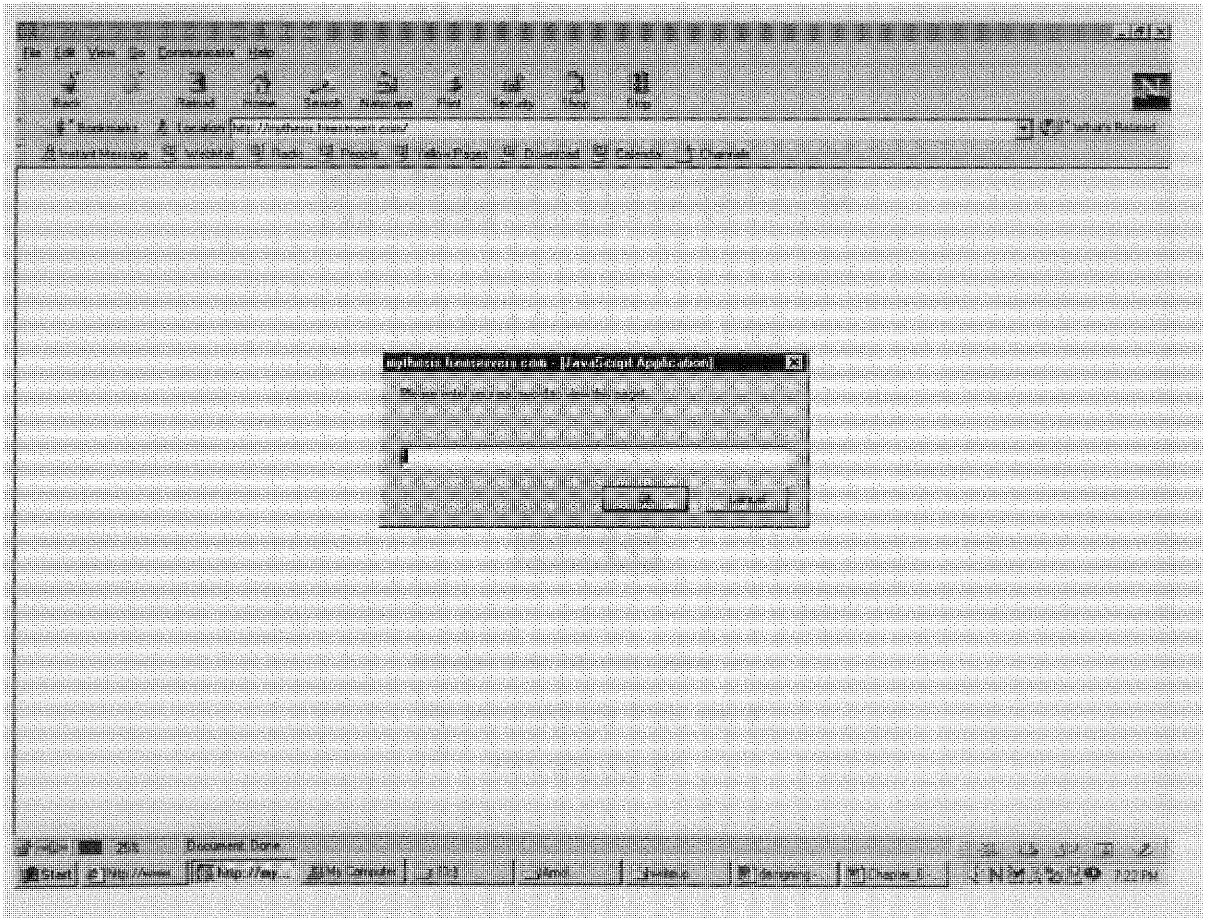
Productivity: Productivity Plug-ins, Map Viewer, Spell Checkers.

VRML/3-D: VRML & QD3D Plug-Ins.

### 6.3 E-Commerce website – Implementation

Due to restrictions in copyrights regarding the E-commerce products, I have taken 20 MB free space from http://www.freeservers.com. I have given my Thesis web server name as http://mythesis.freeservers.com.

Here when you type http://mythesis.freeservers.com you will get the pop up screen which will ask to enter password to enter that web site. This is as shown in figure 6.2 .



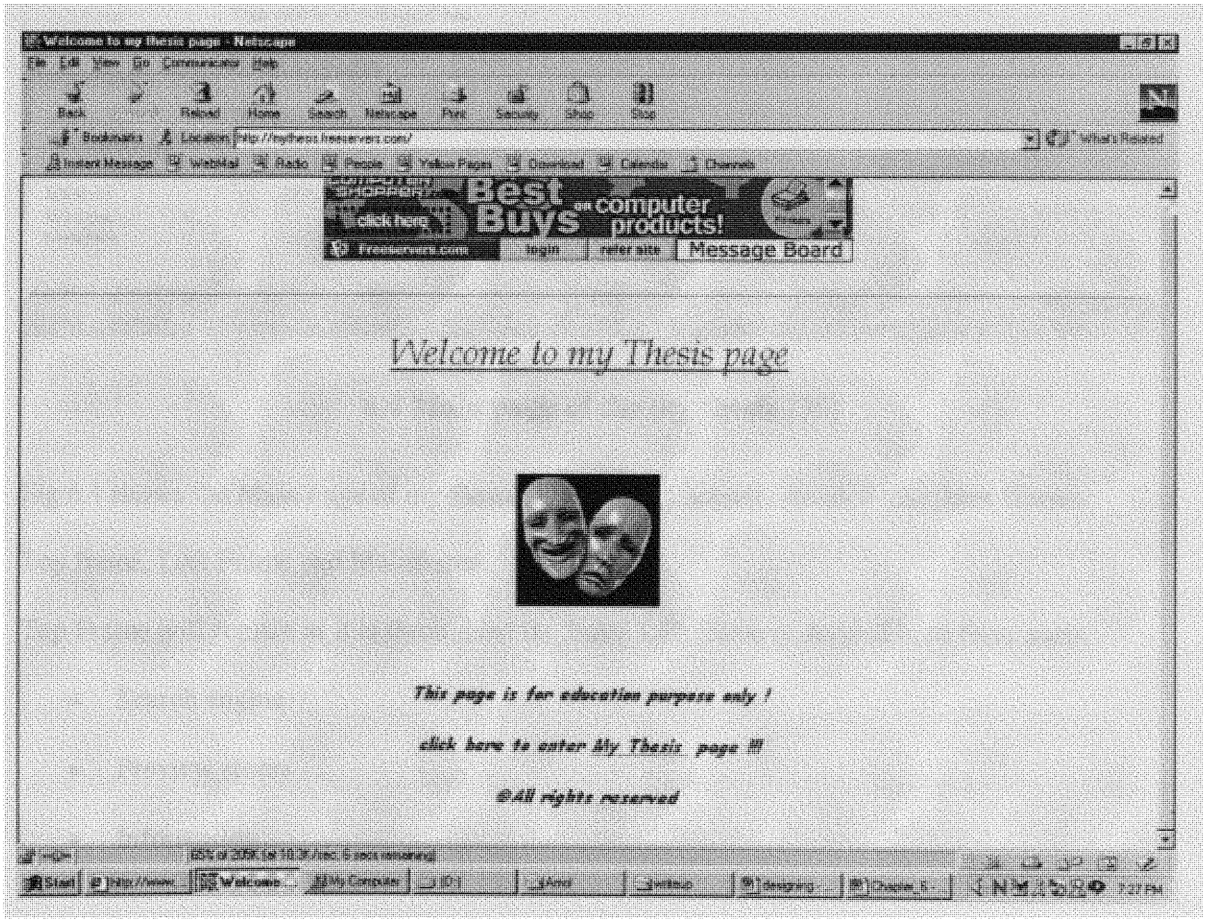
Please enter your password to view this page!

**6.2 Starting page [35]**

As this site I have prepared totally for education purpose I have given this option.

So that only people who is having the password can enter this site.

After entering the password you will get the page as shown in the figure 6.3 this is a just introductory page, which is clearly mentioning that this site is entirely for education purpose. In this page if your mouse cursor passes through or on the text " Welcome to my Thesis page " then automatically the wave file will be played. This I have done with the help of DHTML.



Welcome to my Thesis page

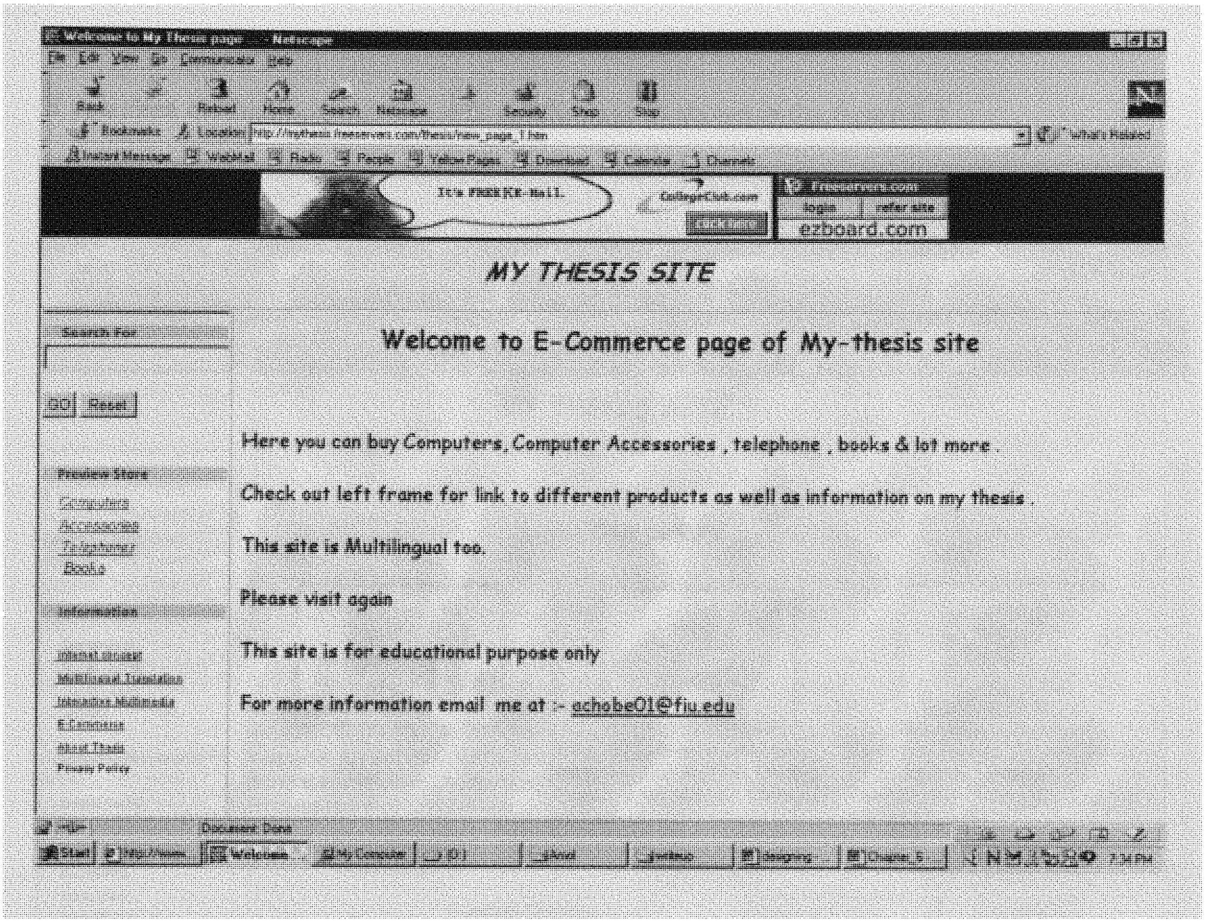
This page is for education purpose only !

click here to enter My Thesis page !!!

©All rights reserved

**6.3 Introductory page [35]**

In this page I have given a link to Main page of my Thesis. If you click that link you will go to Main Page of my thesis.



MY THESIS SITE

Welcome to E-Commerce page of My-thesis site

Here you can buy Computers, Computer Accessories , telephone , books & lot more .

Check out left frame for link to different products as well as information on my thesis .

This site is Multilingual too.

Please visit again

This site is for educational purpose only

For more information email me at :- achobe01@fiu.edu

**6.4 Main page of the my thesis [35]**

Fig 6.4 shows the Main Page of my thesis. This page is actually divided into three frames.

Top frame, Left Frame and Mainframe.

Top Frame will remain as it is throughout the links. Left frame is divided in to three parts.

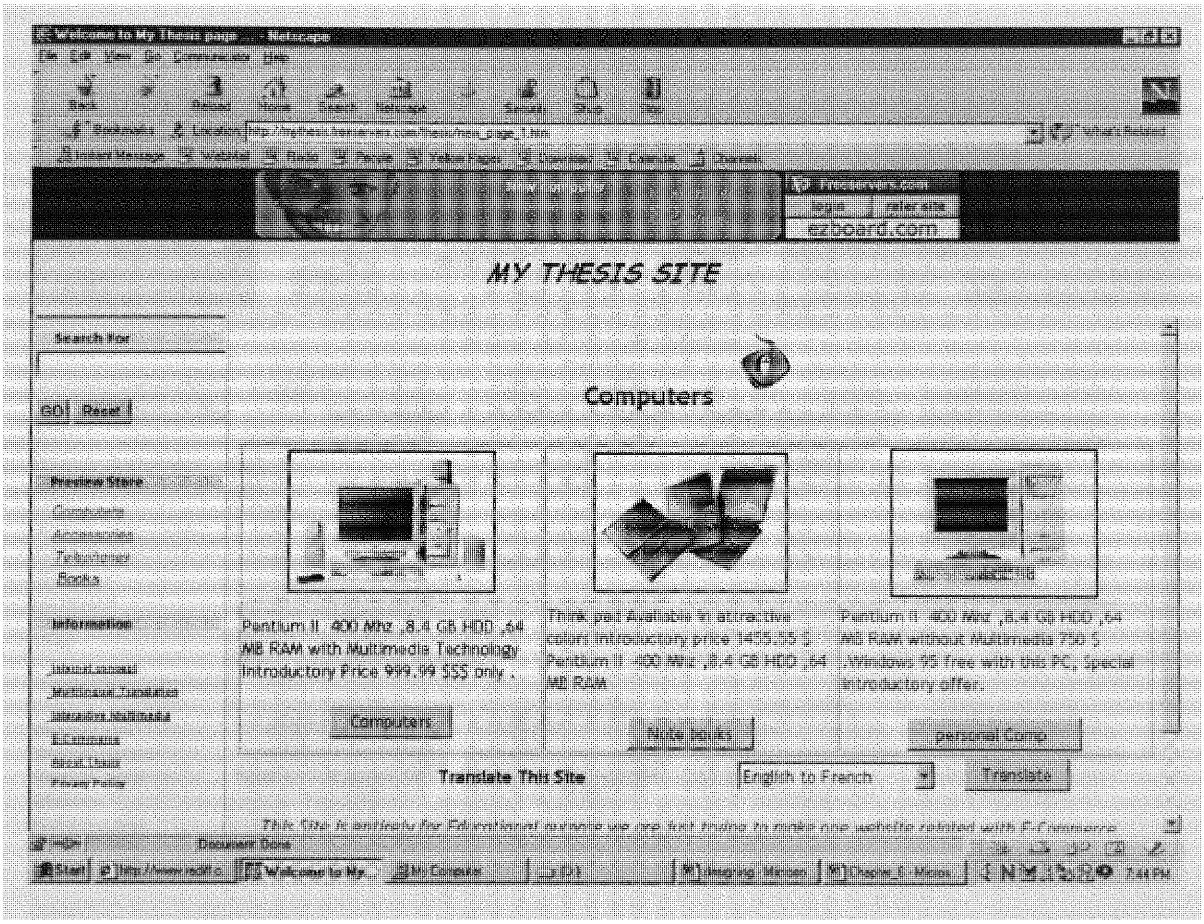
- Search engine
- Preview stores
- Information

Search engine can be used to find the stuffs quickly.

Preview stores section is having 4 different things in that Computers, Accessories , Telephones , books .

This Preview stores is basically having the E-Commerce related stuffs.

If you click on the Computer you will get the page as shown in the figure 6.5.



Pentium II 400 Mhz ,8.4 GB HDD ,64 MB RAM with Multimedia Technology Introductory Price 999.99 $$$ only .

Think pad Available in attractive colors Introductory price 1455.55 $ Pentium II 400 Mhz ,8.4 GB HDD ,64 MB RAM

Pentium II 400 Mhz ,8.4 GB HDD ,64 MB RAM without Multimedia 750 $ .Windows 95 free with this PC, Special introductory offer.

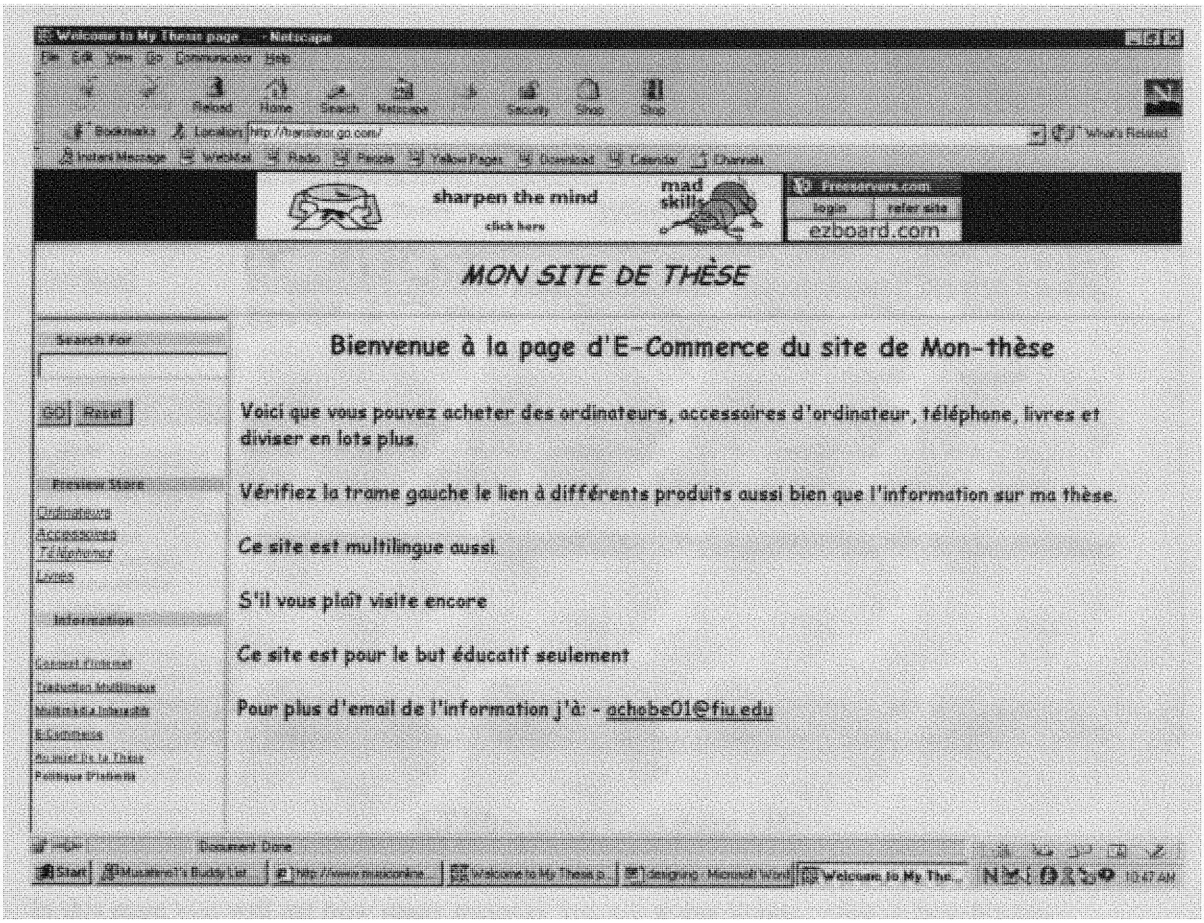
This Site is entirely for Educational purpose we are just trying to make one website related with E-Commerce

**6.5 Trading page [35]**

Only the main frame page is changed to the computer page. Left & top frame as it is.

Here in this Computer page you will find the Computers, Notebooks and personal comp for sale with the brief information about that product. Now if you want to buy say Notebook you are going to click on Notebook bar. This will take you directly to the Shopping cart. Here the most interesting part of the thesis came if the User doesn't know English very well then on this page there is an option that "Translate this site ". This Translation option is for 5 different languages French, Spanish, Portuguese, German, and Italian.

If you click on that option of English to French option then the site will be translate entirely into French Language as shown in the figure 6.6.



MON SITE DE THÈSE

Bienvenue à la page d'E-Commerce du site de Mon-thèse

Voici que vous pouvez acheter des ordinateurs, accessoires d'ordinateur, téléphone, livres et diviser en lots plus.

Vérifiez la trame gauche le lien à différents produits aussi bien que l'information sur ma thèse.

Ce site est multilingue aussi.

S'il vous plaît visite encore

Ce site est pour le but éducatif seulement

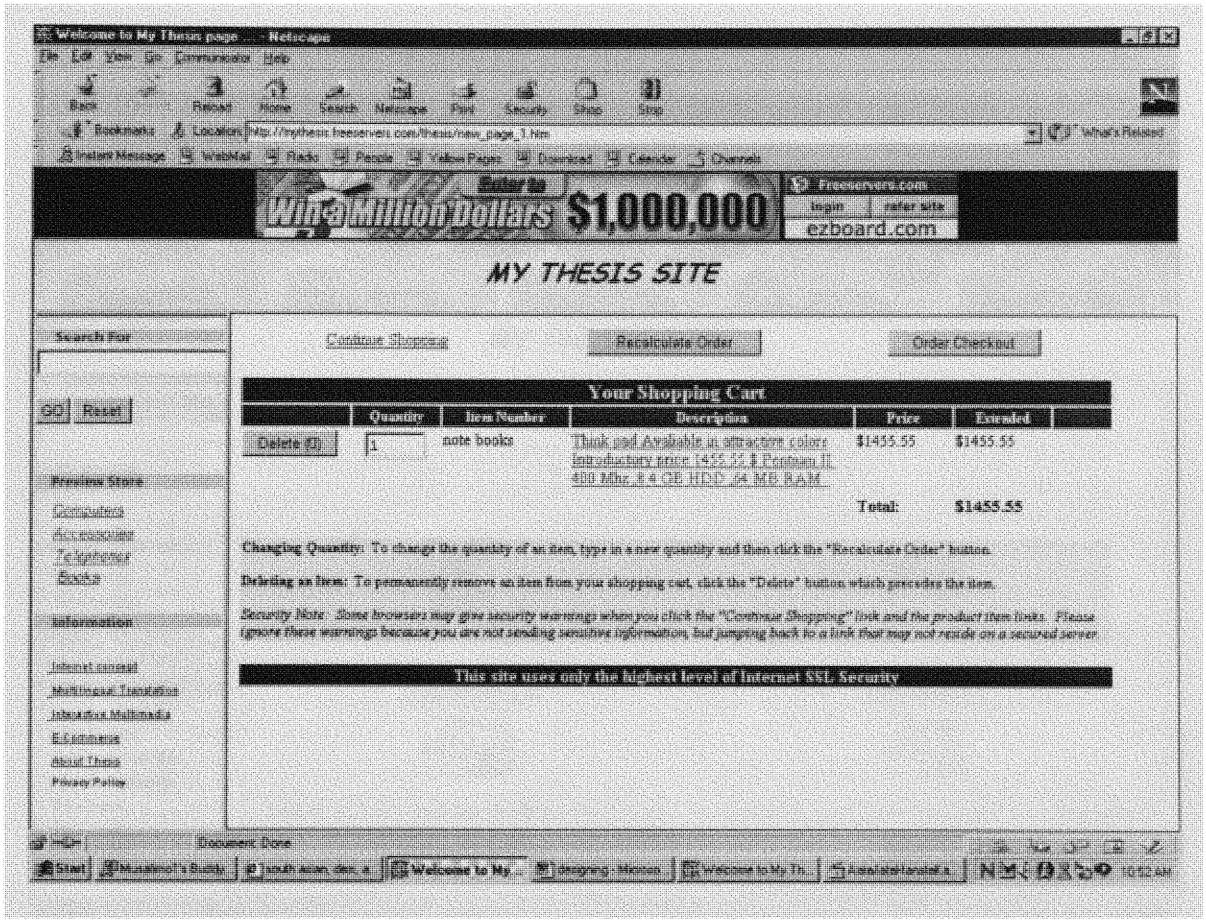
Pour plus d'email de l'information j'à: - achobe01@fiu.edu

6.6 Translation page [35]

After Translation it would go to Main page of the site and you will see all the text has been transferred in French Language.

You can do same thing for Spanish, Portuguese, Italian and German Language.

Now again back to E-Commerce Stuffs. Now in Computer section if you want to buy the Notebook you are just going to Click on the Notebook bar This will take you automatically to Shopping cart page as shown in the figure 6.7.


Welcome to My Thesis page - Netscape
File Edit View Go Communicator Help
Back Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://mythesis.freeservers.com/thesis/new_page_1.htm
What's Related
Instant Message WebMail Radio People Yellow Pages Download Calendar Channels
Enter to Win a Million Dollars $1,000,000
Freeservers.com
login refer site
ezboard.com
MY THESIS SITE
Search For
GO Reset
Previous Store
Computers
Accessories
Telephones
Books
Information
Internet concept
Multilingual Translation
Interactive Multimedia
E-Commerce
About Thesis
Privacy Policy
Continue Shopping
Recalculate Order
Order Checkout
Document: Done
Start

Your Shopping Cart

| | Quantity | Item Number | Description | Price | Extended |
|---|---|---|---|---|---|
| Delete (1) | 1 | note books | Think pad Available in attractive colors Introductory price 1455.55 $ Pentium II 400 Mhz 8.4 GB HDD 64 MB RAM | $1455.55 | $1455.55 |
| | | | | Total: | $1455.55 |

**Changing Quantity:** To change the quantity of an item, type in a new quantity and then click the "Recalculate Order" button.

**Deleting an Item:** To permanently remove an item from your shopping cart, click the "Delete" button which precedes the item.

*Security Note: Some browsers may give security warnings when you click the "Continue Shopping" link and the product item links. Please ignore these warnings because you are not sending sensitive information, but jumping back to a link that may not reside on a secured server*

This site uses only the highest level of Internet SSL Security

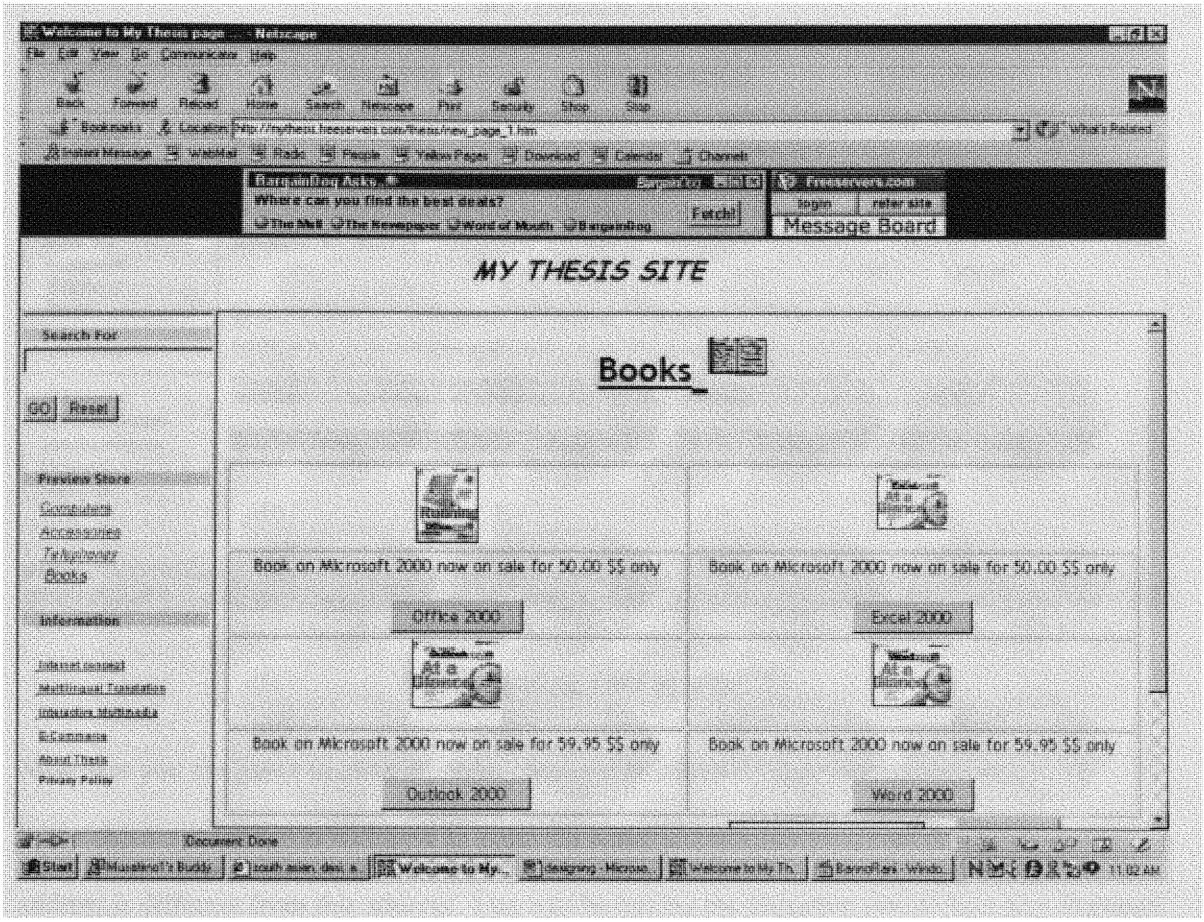
6.7 Shopping Cart page [35]

In this page you will get how many quantity you are going to buy, what is Item Number Description of that Item, Price of that Item. Here you will have three options Continue Shopping, Recalculate Order & Order Checkout.

Continue shopping will allow you to continue the shopping. Recalculate order will recalculate everything and order checkout option is for checking out the order.

Now in this case suppose if you want to buy one book also you are going to click on the Continue Shopping. This page will again take you to the Computer Page. Now you want to buy a book you are going to click on the book on left frame of the page.

Book page is as shown in the fig 6.8.



Welcome to My Thesis page - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://mythesis.freeservers.com/thesis/new_page_1.htm
What's Related
Instant Message WebMail Radio People Yellow Pages Download Calendar Channels
BargainDog Asks...
Where can you find the best deals?
The Mall The Newspaper Word of Mouth BargainDog
Fetch!
Freeservers.com
login refer site
Message Board
MY THESIS SITE
Search For
GO Reset
Preview Store
Computers
Accessories
Telephones
Books
Information
Internet request
Multilingual Translation
Interactive Multimedia
E-Commerce
About Thesis
Privacy Policy
Books
Office 2000
Excel 2000
Outlook 2000
Word 2000
Document: Done
Start

Book on Microsoft 2000 now on sale for 50.00 $$ only

Book on Microsoft 2000 now on sale for 50.00 $$ only

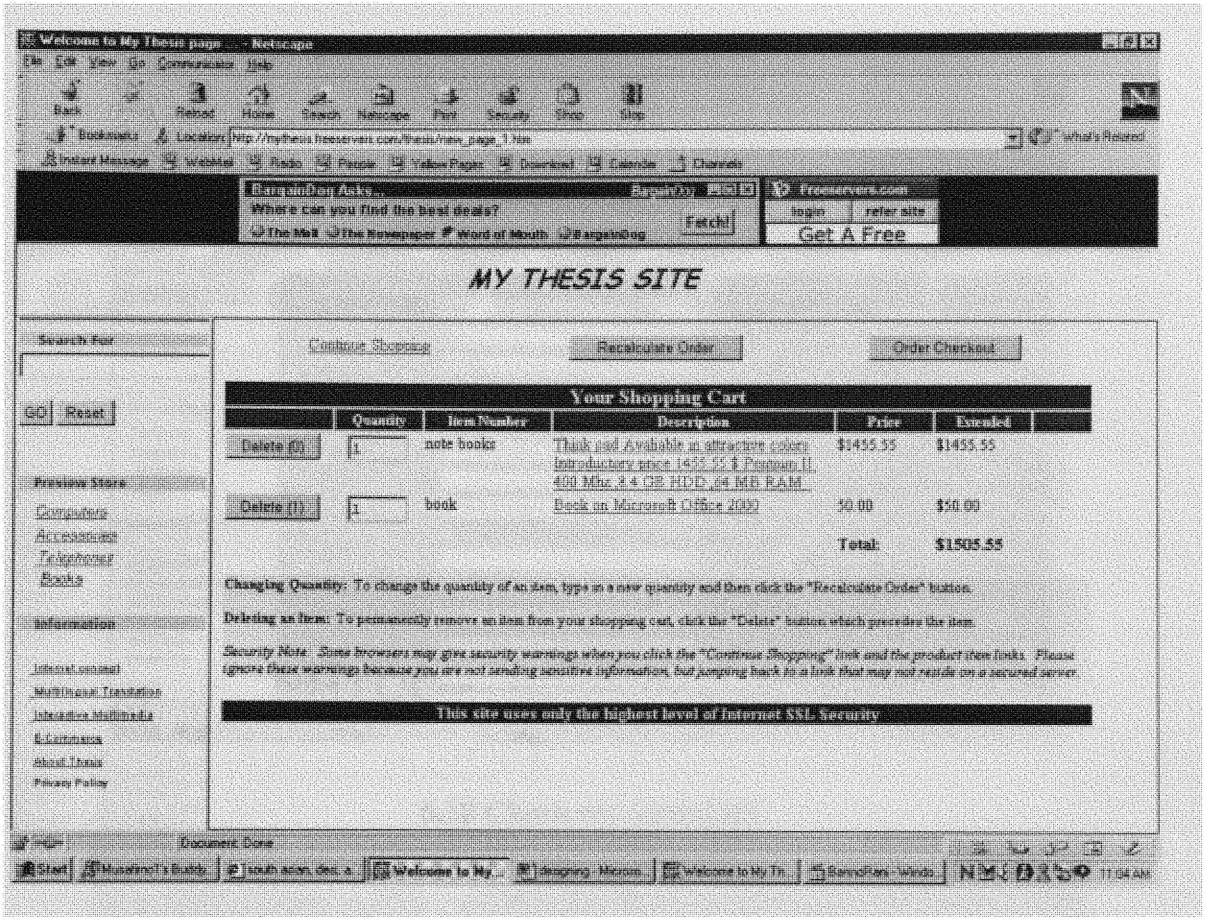
Book on Microsoft 2000 now on sale for 59.95 $$ only

Book on Microsoft 2000 now on sale for 59.95 $$ only

**6.8 Books page [35]**

Now if you want to buy Office 2000 book you are going to click on Office 2000 bar.

This will make your shopping cart page as shown in Fig 6.9.



Your Shopping Cart

| | Quantity | Item Number | Description | Price | Extended |
|---|---|---|---|---|---|
| Delete (0) | 1 | note books | Think pad Available in attractive colors Introductory price 1455.55 $ Pentium II 400 Mhz 4.4 GB HDD 64 MB RAM | $1455.55 | $1455.55 |
| Delete (1) | 1 | book | Book on Microsoft Office 2000 | 50.00 | $50.00 |
| | | | | Total: | $1505.55 |

**Changing Quantity:** To change the quantity of an item, type in a new quantity and then click the "Recalculate Order" button.

**Deleting an Item:** To permanently remove an item from your shopping cart, click the "Delete" button which precedes the item.

*Security Note: Some browsers may give security warnings when you click the "Continue Shopping" link and the product item links. Please ignore these warnings because you are not sending sensitive information, but jumping back to a link that may not reside on a secured server.*

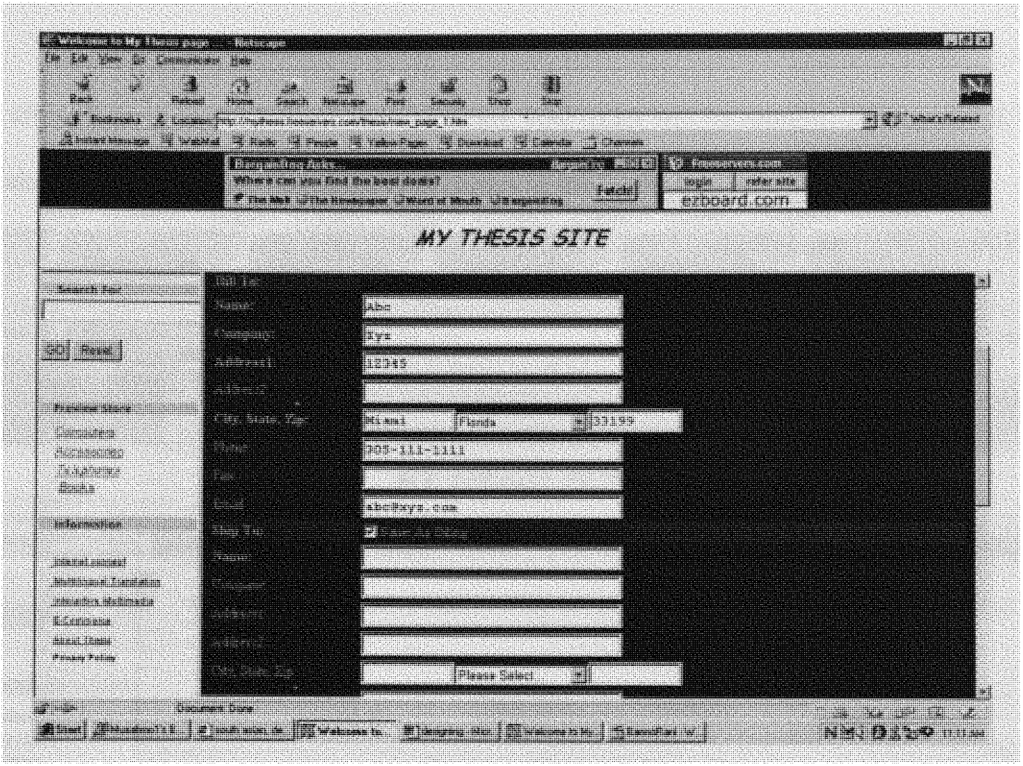
This site uses only the highest level of Internet SSL Security

### 6.9 Shopping cart again [35]

Now here you are going to click on order checkout to complete this buying process.

In the check out form you will have to write the name address, telephone no & if the Shipping address is different from this address. You will be having the Shipping option here like Standard option, second day & overnight delivery. The Form is as shown in the Figure 6.10.

After filling out this form it will take you to Confirm & submit order page here you will be having the total amount. This is shown in the figure 6.11.

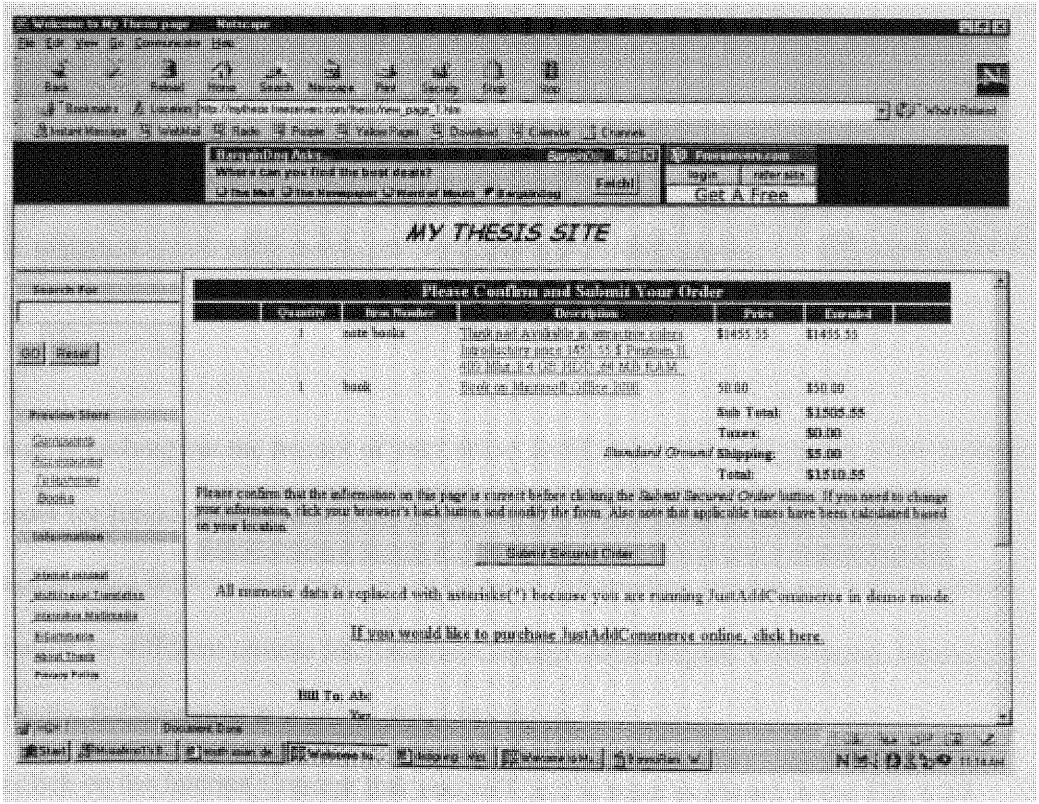


Welcome to My Thesis page ... - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://mythesis.freeservers.com/thesis/new_page_1.htm
What's Related
BargainDog Asks...
Where can you find the best deals?
The Mall The Newspaper Word of Mouth BargainDog
Fetch!
Freeservers.com
login refer site
ezboard.com
Search For:
GO Reset
Preview Store
Computers
Accessories
Telephones
Books
Information
Internet concept
Multilingual Translation
Interactive Multimedia
E-Commerce
About Thesis
Privacy Policy
Document: Done

MY THESIS SITE

| | | | |
|---|---|---|---|
| Bill To: | | | |
| Name: | Abc | | |
| Company: | Xyz | | |
| Address1: | 12345 | | |
| Address2: | | | |
| City, State, Zip: | Miami | Florida | 33199 |
| Phone: | 305-111-1111 | | |
| Fax: | | | |
| Email: | abc@xyz.com | | |
| Ship To: | ☑ Same As Billing | | |
| Name: | | | |
| Company: | | | |
| Address1: | | | |
| Address2: | | | |
| City, State, Zip: | | Please Select | |

6.10 Check out form [35]



Welcome to My Thesis page ... - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://mythesis.freeservers.com/thesis/new_page_1.htm
What's Related
BargainDog Asks...
Where can you find the best deals?
The Mall The Newspaper Word of Mouth BargainDog
Fetch!
Freeservers.com
login refer site
Get A Free
Search For:
GO Reset
Preview Store
Computers
Accessories
Telephones
Books
Information
Internet concept
Multilingual Translation
Interactive Multimedia
E-Commerce
About Thesis
Privacy Policy
Document: Done

MY THESIS SITE

Please Confirm and Submit Your Order

| Quantity | Item Number | Description | Price | Extended |
|---|---|---|---|---|
| 1 | note books | Think pad Available in attractive colors Introductory price 1455.55 $ Pentium II 400 Mhz,4.4 GB HDD,64 Mb RAM. | $1455.55 | $1455.55 |
| 1 | book | Book on Microsoft Office 2000 | $50.00 | $50.00 |
| | | | Sub Total: | $1505.55 |
| | | | Taxes: | $0.00 |
| | | *Standard Ground* | Shipping: | $5.00 |
| | | | Total: | $1510.55 |

Please confirm that the information on this page is correct before clicking the *Submit Secured Order* button. If you need to change your information, click your browser's back button and modify the form. Also note that applicable taxes have been calculated based on your location.

Submit Secured Order

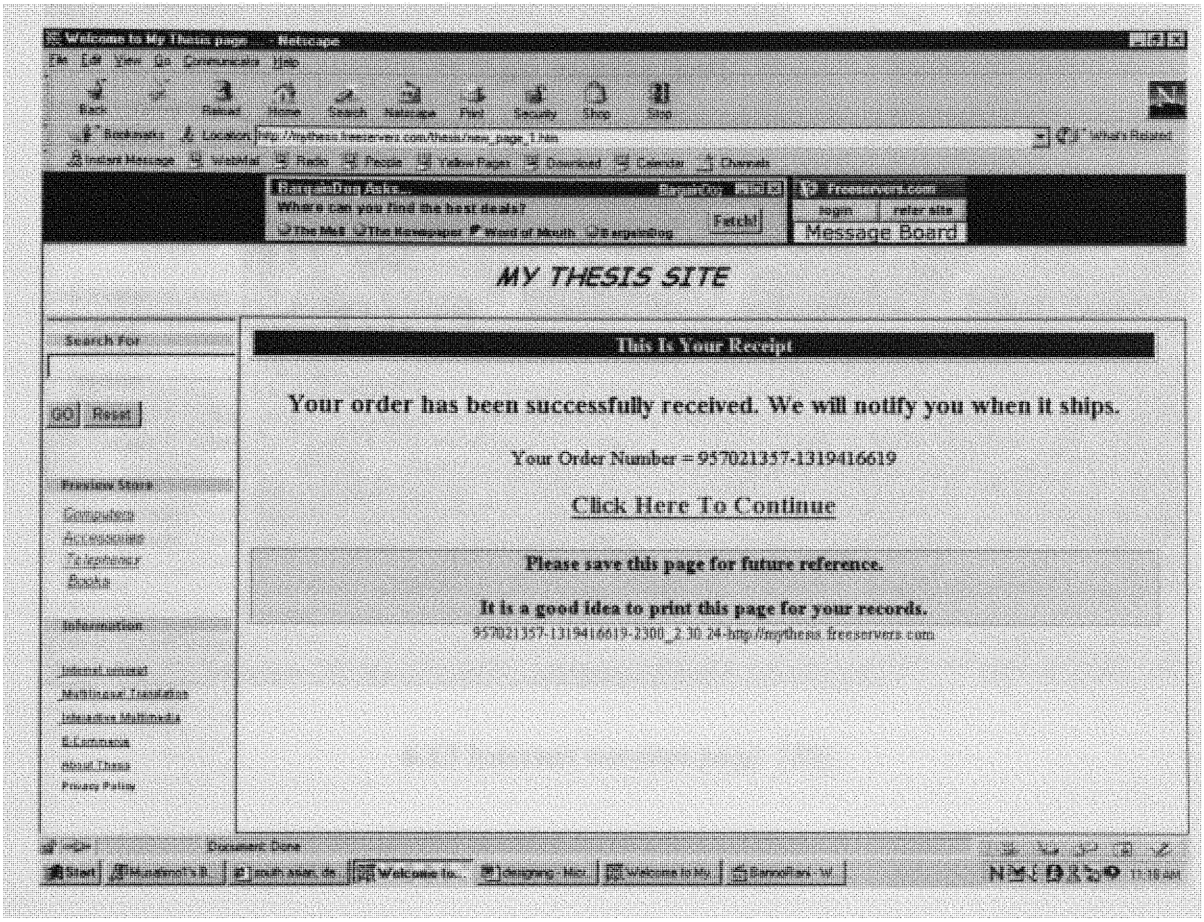
All numeric data is replaced with asterisks(*) because you are running JustAddCommerce in demo mode.

If you would like to purchase JustAddCommerce online, click here.

Bill To: Abc
Xyz

6.11 Submission form page [35]

Here after clicking on the Submit Secured order, your order will be submitted to my site & this will take you to new page. This page is as shown in the figure 6.12.



This Is Your Receipt

Your order has been successfully received. We will notify you when it ships.

Your Order Number = 957021357-1319416619

Click Here To Continue

Please save this page for future reference.

It is a good idea to print this page for your records.

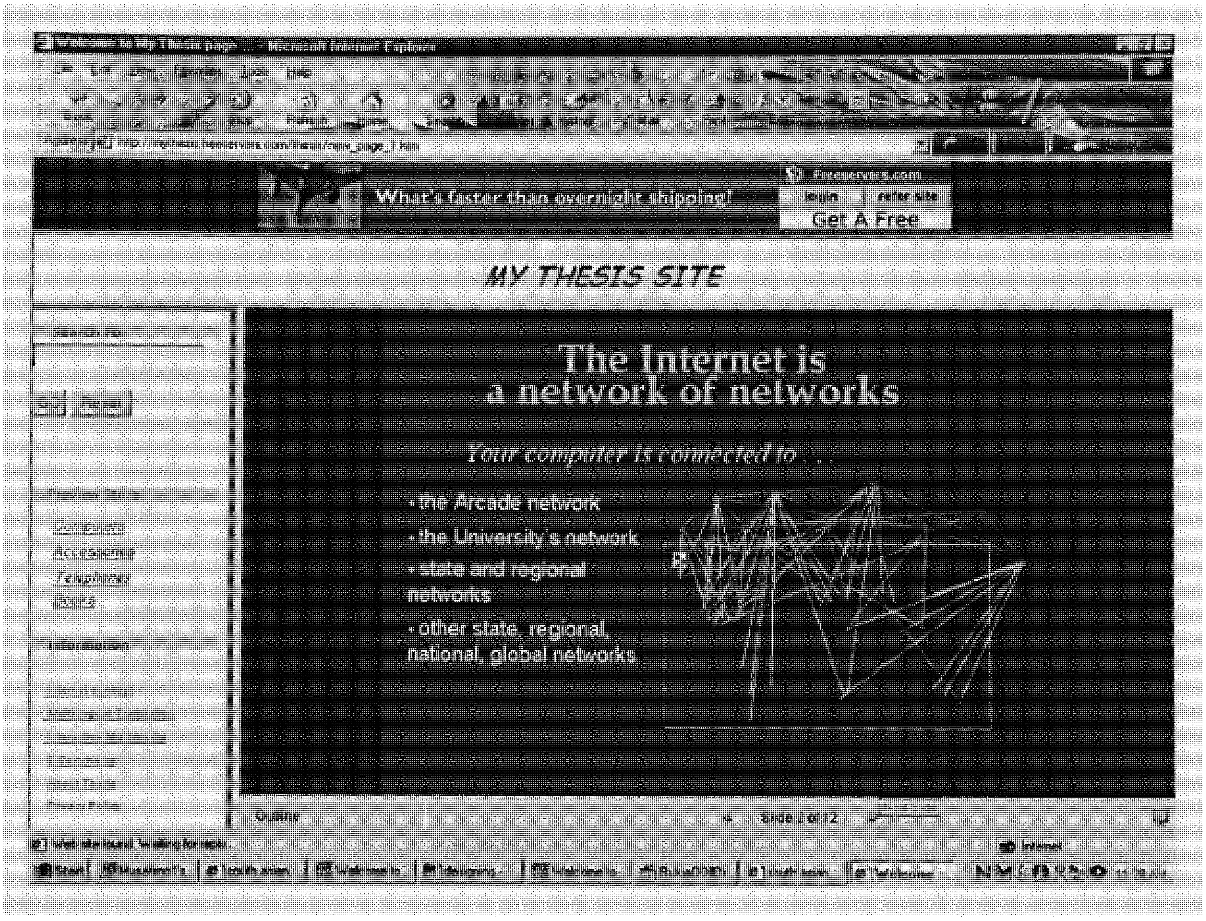
957021357-1319416619-2300_2 30 24-http://mythesis.freeservers.com

6.12 Final Receipt [35]

This page is nothing but the receipt of your order. In this page you will get the order number of your order for future reference.

Now again going back to main page in left frame in Information section you will be having Information on different articles like Internet Concept, Multilingual Translation, Interactive Multimedia, E-Commerce & a article about My thesis.

If you click on the Internet Concept link you will get the page as shown in the Fig. 6.13



Welcome to My Thesis page ... - Microsoft Internet Explorer

What's faster than overnight shipping?

MY THESIS SITE

The Internet is
a network of networks

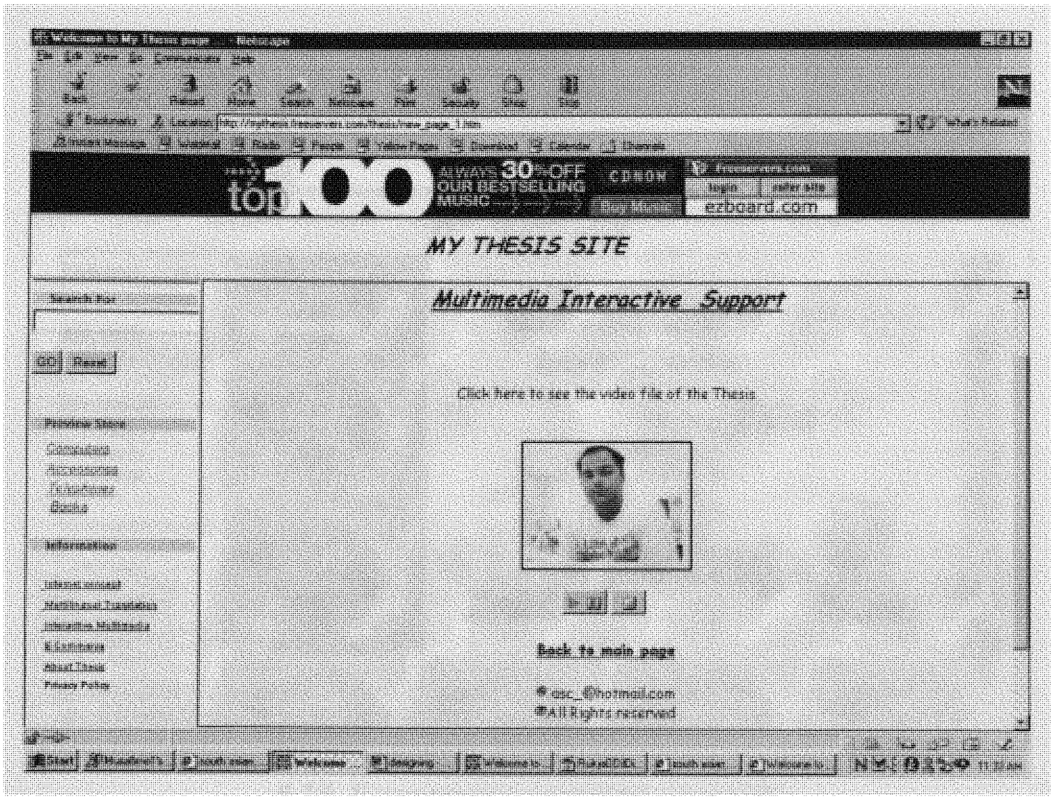
*Your computer is connected to . . .*

- the Arcade network
- the University's network
- state and regional networks
- other state, regional, national, global networks

**6.13 Internet concept page [35]**

Here you are having different slides about the Internet Concept.

In the Left frame window if you click on the Multilingual Translation you will get the link to the page where you can translate the web site as well as text in different languages .in the left frame if you click on Interactive multimedia you will get link to page where I have put the video file which automatically play in Real Video mode, This video gives information about my thesis, this is shown in the figure 6.14.



MY THESIS SITE

Multimedia Interactive Support

Click here to see the video file of the Thesis

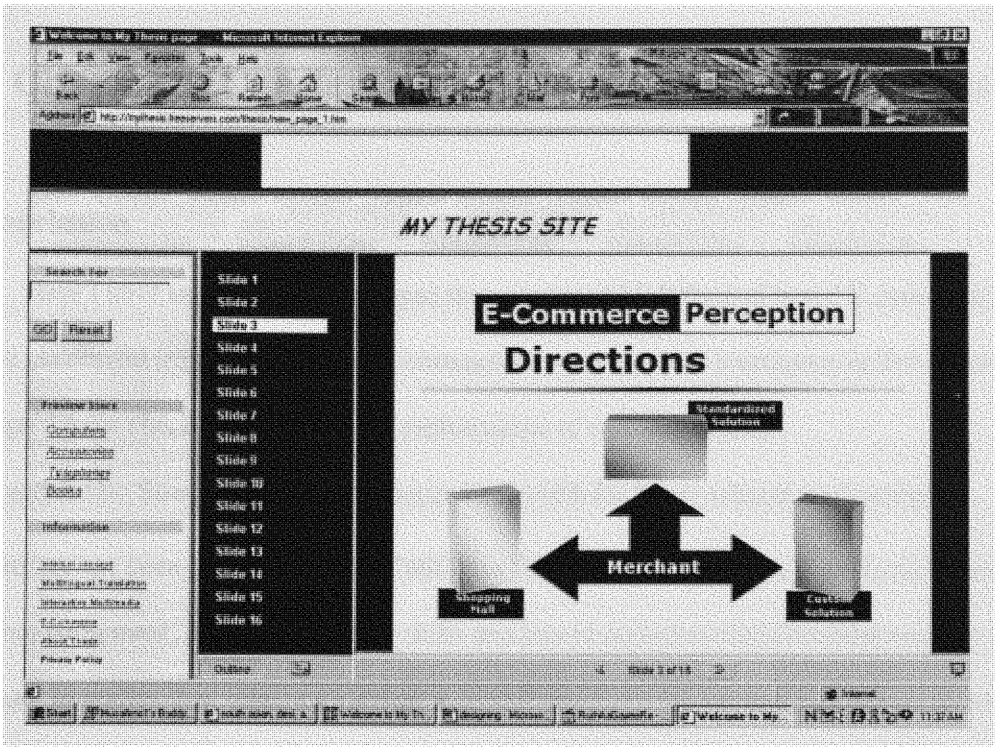
Back to main page

© osc_@hotmail.com
©All Rights reserved

**6.14 Real video file [35]**

If you click on E-Commerce link in left frame window this will take to a page where the slides of E-commerce concept are there. This is shown in the Figure 6.15.

Here there are 16 different slides, which gives information on the E-commerce.



**6.15 E-commerce overview page [35]**

Now in the about thesis link I have given a brief introduction about my thesis.

# Chapter 7: Conclusions and Future Recommendations

## 7.1 Conclusion

Here I have successfully developed the concept of Multilingual based E-commerce & also the successful implementation of E-commerce site along with translation in five different language .I have checked for successful performance of web server also.

Video and Audio Streaming requires a better bandwidth for hyper critical application

The Internet has been compared to the California Gold Rush of 1849. For a moderate investment in mining equipment, a person with few skills and lots of ambition could become wealthy overnight. In reality, few miners scratched a good living from the streams and rivers, fewer still struck it rich. There were, however, amazing success stories such as Levi Strauss and Paul Armour, who both built Fortune 500 companies from modest beginnings of supplying miners with clothing and meat.

The Internet, and specifically electronic commerce (e-commerce), offers the same tantalizing promise; for the price of an Internet account and a free Web server, a person with few skills and lots of ambition can become wealthy by setting up shop to sell merchandise. However, few businesses are making a success this way.

In the mid-1850s, large mining companies with the right equipment and skills began removing large amounts of gold from the hills and rivers in California. Miners abandoned their claims to work for the mining companies. By applying technology and skills to gold mining, the miners were making money. The mining companies grew rich.

We're seeing the same shift in e-commerce. Businesses with the tools, skills, and direction are creating e-commerce sites and making them a success. Pioneers like Egghead.com and Bank of Montreal helped define the technology requirements, and refine the needed skills for e-commerce.

E-commerce is not new. Using electronic data interchange (EDI), companies such as Ford Motor Company and Wal-Mart have been trading purchase orders and invoices electronically for years. Information services such as Lexis-Nexus and Dialog have allowed customers to order and buy research materials and databases through private dial-up lines and a proprietary application. E-commerce provided these companies, and others like them, with an edge over their competition; doing business electronically is often faster, cheaper, and more efficient than working with paper. The Internet opens the world of e-commerce to every company by replacing private - and expensive - phone lines with a public network that anyone with a computer and modem can access. It provides companies with a standard interface, making e-commerce applications easier for customers to use. And it offers global access for the price of a local phone call.

Surprisingly, only about 4 percent of companies on the Internet are using it for commerce today. Every company has the opportunity to become the Levi Strauss or Paul Armour of the Internet, building both an opportunity and a competitive advantage.

**What is E-Commerce?**

While we tend to think of e-commerce as online shopping, it is actually any transaction that occurs over two computer systems.

International banking firm Piper Jaffray conservatively estimates that the entire e-commerce marketplace will reach $228 billion by 2001. Price Waterhouse projects trading in goods and services online will generate $434 billion by 2002, and Activmedia estimates total e-commerce revenue to reach $1 trillion by 2001.

This "entire marketplace" is made of several types of online transactions:

Consumer purchases - Home shoppers will spend $54 million by 2002; this is more than 10 times the $4.3 million spent in 1997. (Web Usage Trends 1998, IDC and RelevantKnowledge)

Business purchases - The business-to-business sector will account for $268 billion, the majority of e-commerce revenue through to 2002. (1998 eCommerce Report, eMarketer)

Online banking - Close to five million people, or 5 percent of the U.S. population, do some form of online banking, but by the end of 2001, that number will go up to about 22 million, or 21 percent of the population. (Online Banking Report)

Bill payment and presentation - One million bills will be presented via the Internet in 1998, growing to 500 million by 2000; this represents about 3 percent of all consumer bills. (BancAmerica)

**Securities trading** - There will be 14.4 million traders on the Internet by 2002, up from three million today. Ameritrade claims their Internet trading accounts have grown from 98,000 to 147,000 in the first fiscal quarter of 1998. (Ameritrade Holding Corp.)

Procurement - A survey among members of the National Association of Purchasing Management (NAPM) said that 55 percent of managers purchased goods directly from a supplier Web site, while 36 percent make orders via intranet-based software. More than 67 percent currently engage in some sort of electronic purchasing, with the number expected to grow to 85 percent within the next six months. (Visa USA)

An e-commerce business usually engages in one or more of the above. For example, a firm may do consumer sales through a Web site, order from their suppliers via EDI, and offer bill payment through electronic funds transfer (EFT). A bank may offer online banking, securities trading, bill payment, and consumer goods, such as concert tickets, transportation passes, and postage stamps. Another aspect of e-commerce is information publishing. Roughly 70 percent of the people on the Internet use it to research product information that they later use to make a buying decision. For instance, automobile manufacturers all offer sites where you can shop for a car, then point you to a dealership to complete the transaction. (Saturn actually allows you to complete the transaction, including financing, online.)

Online businesses are also users of e-commerce. Studies show that the people most comfortable buying online are those who also sell online.

## Benefits of E-commerce

Consulting firm Booz-Allen & Hamilton studied several different types of businesses doing standard business transactions over the Web. They found that the Internet had tremendous impact on the cost structure of the business model. For example:

The banking industry today spends about $1.08 to perform a simple teller transaction at the branch. Each newer technology has reduced this cost by half: Banking by phone, followed by personal computer (PC) banking, followed by the current choice of doing the same transaction on the Web. This same transaction has been reduced during this time from $1.08 to 13 cents.

The costs for issuing an airline ticket can be reduced from $8 to $1 over the Web.

The retail sales cost in a brick- and-mortar store is at least $12 per transaction; based on the store's cost structure, it may be higher. Telesales can cost between $5 and $7. Selling on the Web reduces the cost to $2 per transaction.

A bill, printed and mailed, costs up to $1.50 for printing, postage, and labor. Add another 10 cents per bill for a lock box. Online billing and payment eliminates all these costs.

Cost cutting is only one reason to move to e-commerce. The Internet also provides a global marketplace with 24x7 operation - and the only marketplace where a small business has an equal footing as a big business. The right equipment and skills allow any business to look like a Fortune 500 corporation.

E-commerce systems help companies stay in touch with their customers. As a customer visits the Web site to place an order, he or she has an opportunity to interact with the company. Through effective use of this opportunity, the company can build loyalty. For example, Amazon.com records purchasing information and suggests books that the customer might like to read. Rage

Systems offers an interactive forum where customers can exchange ideas. Nua Research consolidates Internet statistics and sends them via e-mail once a week.

A well-designed e-commerce site can augment your company's sales force. Through Web-only contact, the visitor can move through the entire Attention, Interest, Desire, and Action (AIDA) process:

Attract Attention to a product or service through an on-site advertisement or e-mail announcement.

Build Interest through forums, online applications, and detailed information.

Create Desire by offering an added value for Internet customers.

Move the visitor to Action with online ordering and payment.

Remarkably, few companies are taking advantage of this opportunity.

## 7.2 Future Recommendation

### Requirements of a Successful E-commerce Network

The following features are considered essential for creating a successful e-commerce network.

**Speed** is of utmost importance in the list of e-commerce requirements. Studies show that Internet users will wait no longer than 30 seconds for a page to load and no longer than two minutes for a system to return information. Internal users want consistency in speed - to know, for instance, that it will always take 10 seconds to retrieve e-mail, not five seconds this time and 70 seconds next time. External customers will not tolerate delays. If they wait too long, they'll move to a competitor's site.

**Security** is a major issue to manage when dealing with the Internet. In spite of a firewall and pass-through to the database and line-of-business applications, there's always a chance that business data will be compromised. Access policies, IP tunneling, IP masking, and encryption are commonly used security measures.

**Reliability** is also essential. Many Internet users are forgiving of occasional outages and down time, but there are too many factors outside of your control that affect this. Internal corporate users, however, are less forgiving. With more vital-to-business information stored on remote servers and applications, downtime - and delay-causing congestion - means an operating loss.

**Scalability** is a requirement from day one. The number of users can never compromise the speed of the e-commerce application. The site you build should have room to grow by a factor or 1,000 as your online business grows; thus, if you are now supporting 100 transactions per day, you should prepare to handle as many as 100,000.

**Ease of management** keeps the network traffic flowing at a smooth pace at all times. Few Internet applications provide tools to measure performance, which is necessary to ensure network efficiency.

## Research to improve the ways we interact with computers

Computers are still too hard to use; surveys show that computer users waste over 12 percent of their time because they can't understand what their computers are doing

Improved accessibility for people without a keyboard (for example, mobile professionals and doctors) and persons with disabilities

Better techniques for locating data and extracting "knowledge" from data Proposed research areas: Computers that speak, listen, and understand human language

Information visualization

### Development of Additional Languages

Development of new language pair translation capability between languages, for which source and target modules task has already done, is the easiest to accomplish. Only a new transfer module and the transfer/target dictionaries need to be created.

Development of additional target language capability for each source system is possible and quite economical because some systems are set up as "Multi-target" systems. Adding another target language would necessitate only the development of a new Transfer module and a new Synthesis module, as well as building up the Transfer / Target dictionaries.

Development of additional source language capability for each target system is more difficult, if a completely new parser has to be created. However, if the new source language is closely related to one of the existing source languages, development of a new parser can take advantage of common rules within a language family via the use of existing "Trunk Parsers", (such as Romance Trunk, Slavic Trunk...).

# References

1. Lynn Margherio, Dave Henry, Sandra Cooke et al., "The Emerging Digital Economy", April 1998
2. Meeker, Mary and Pearson, Sharon "Morgan Stanley U.S. Investment Research: Internet Retail", Morgan Stanley, May 28, 1997
3. Nicholas Negroponte, founder and director of the MIT Media Lab, estimates that 1 billion people will use the Internet as early as 2000. Source: "The Third Shall Be First: The Net leverages latecomers in the developing world." Wired, January 1998.
4. IntelliQuest estimates 62 million online in the United States in the 1997. IntelliQuest, IntelliQuest Press Release February 4, 1998. http://www.intelliquest.com/about/release41.htm
5. Inktomi Corporation White Paper 1997. Available online at http://www.inktomi.com/Tech/EconOfLargeScaleCache.html
6. Network Wizards "Internet Domain Survey." http://www.nw.com/
7. Consumer Electronics Manufacturers Association (CEMA). "U.S. Consumer Electronics Industry Today." June 1997, pp. 50-52. CEMA reports that 40 percent of U.S. households own PCs. A more recent analysis by IDC/Link estimates that the penetration rate has now reached 43 percent.
8. While high-speed optical fiber lines are used for long-distance communications, most U.S. homes connect to these lines via lower-bandwidth copper wire. Integrated Services Digital Network (ISDN) connections have become widely available to households and businesses, but a very small percentage of Internet subscribers use them.
9. Federal Communications Commission (FCC), "Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming", CS Docket No. 96-496. January 2, 1997. pp.58-59. http://www.fcc.gov/Bureaus/Cable/Reports/fcc97423.html
10. *Marshall Brain* ,"How E-commerce works" http://www.howstuffworks.com/ecommerce9.htm
11. Global Internet Statistics the latest estimated figures of the number of each online language population, http://www.euromktg.com/globstats
12. Article on "How to Approach E-commerce in Europe and Latin America" http://www.glreach.com/eng/ed/art/rep-eur13.html
13. Constance H. McLaren, Bruce J., "E-commerce: business on the Internet ", Cincinnati: South-Western Educational Pub , 2000 .
14. http://www.emarketer.com/
15. Marshall Brain, "How E-Commerce works" http://www.howstuffworks.com/ecommerce6.htm
16. Marshall Brain, "How E-Commerce works" http://www.howstuffworks.com/ecommerce8.htm

17. Gangawani, Garg, Jayanthy KR "E-commerce development: business to consumer " Redmond, Wash.: Microsoft Press, 1999

18. Andrew S. Tanenbaum, "Computer Networks," 3rd edition, Prentice Hall, March 1996

19. Fred Halsall, "Data Communications, Computer Networks and Open Systems," 4th edition, Addison Wesley Longman, Inc., September 1995

20. Deborah Russell , G.T.Gangemi , "Computer Security Basics" 3rd edition O'Reilly & Associates , January 1999

21. Article about Secure Socket Layer by Netscape, "How SSL works " http://developer.netscape.com/tech/security/ssl/howitworks.html

22. Christina Schaffner, "Translation and Norms, " Clevedon, England, January , 1999

23. Machine Translation: Past, Present, Future" http://www.systransoft.com/Papers/ppr_mt4a.htm

24. Enterprise Translation Server web site Product description article http://www.transparentlanguage.com/ets/about/intro.htm

25. Enterprise Translation Server web site article about translation of website http://www.transparentlanguage.com/ets/about/htmlwebpages.htm

26. Keith Schengili-Roberts, Kim Silk-Copeland, " The Advanced Html Companion " Morgan Kaufmann Publishers, August, 1998

27. Jeffrey C. Rice, Irving, III Salisbury, "Advanced Java 1.1 Programming" Computing McGraw-Hill, August 1997

28. Site having information about Just add Commerce Software http://www.richmediatech.com/msportal.html

29. Fcc, CS Docket no. 96-496, 19976; "ADSL from werbach " 1997, p.75

30. General site about information, "What is E-commerce " http://www.whatis.com

31. General search engine site, "Tutorial on web site" http://www.askjeeves.com

32. General Information related site about Information technology , http://www.learnthenet.com

33. Article on Internet security by Petri Japilla, Pettri Poyhonen, "The Internet Security", PDF file .

34. Global reach website Internet online marketing analysis http://www.glreach.com/index.php3

35. Thesis title "Multilingual Interactive Multimedia Based E-Commerce" website by Amol Chobe, http://mythesis.freeservers.com