



University of Nebraska at Omaha
DigitalCommons@UNO

Student Work

1-1-2003

Survey on E-commerce and its applications

Zhenhua Gu

University of Nebraska at Omaha

Follow this and additional works at: <https://digitalcommons.unomaha.edu/studentwork>

Recommended Citation

Gu, Zhenhua, "Survey on E-commerce and its applications" (2003). *Student Work*. 1311.
<https://digitalcommons.unomaha.edu/studentwork/1311>

This Thesis is brought to you for free and open access by DigitalCommons@UNO. It has been accepted for inclusion in Student Work by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.



SURVEY ON E-COMMERCE AND ITS APPLICATIONS

A Thesis

Presented to the

Department of Computer Science

and the

Faculty of the Graduate College

University of Nebraska

in Partial Fulfillment

of the Requirements for the Degree

Master of Science

University of Nebraska at Omaha

by

Zhenhua Gu

January, 2003

UMI Number: EP73451

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI EP73451

Published by ProQuest LLC (2015). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code

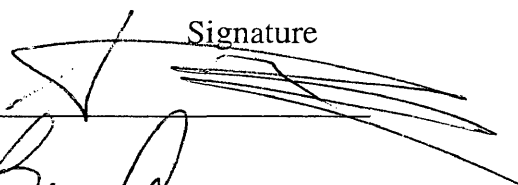
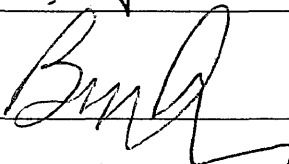


ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

THESIS ACCEPTANCE

Acceptance for the faculty of the Graduate College,
University of Nebraska, in partial fulfillment of the
requirements for the degree of Master of Science,
University of Nebraska at Omaha.

Committee

Name	Signature
Dr. A. D. STOYEN	
Bing Chen	
PETER A. NG	P. A. Ng

Chairperson (signature) P. A. Ng Date Jan 16, 2003

Co-Chairperson (signature) _____ Date _____

(if applicable)

SURVEY ON E-COMMERCE AND ITS APPLICATIONS

Zhenhua Gu, MS

University of Nebraska, 2003

Advisor: Peter A. Ng, Professor

Electronic Commerce, usually is called e-commerce, conducts business on-line. It is electronic forms of communication that permits the exchange of sale information related to goods and services purchasing between buyers and sellers with digital cash and via Electronic Data Interchange (EDI). The application of e-commerce is very important because that is the only way that how buyers and on-line business stores make the deals without seeing and talking each other. The applications should be very friendly (interface with nice layout and easily accepted by the potential buyers), easy to access and use (almost without to learn any computer and network skills), showing all the necessary and related information to all the viewers (no any questions could not be found during purchasing), and trusted by real buyers (secure without the personal information leaking to third party especially social secure number and financial information). The well know on-line solutions are from IBM's WebSphere Commerce Suite, Microsoft Corp's Site Server Commerce Edition, Yahoo's Yahoo Store, and BroadVision's One-to-One Commerce, and all of them use web secure protocols such as S-HTTP (Secure HyperText

Transfer Protocol), SSL (Secure Sockets Layer), or SEPP (Secure Electronic Payment Protocol). E-commerce has a lot of benefits if it compares with long time traditional business – less expense, space saving, spread fast, saving shopping time, easy comparison, almost no sales tax, etc.. With Internet and personal computer growing dramatically in the last decade, we already saw the huge on-line business obviously. In the next few years along with technological development and innovation of computer, Internet, and any other related factors, the potential e-commerce market will grow to billion and billion dollars business worldwide. E-commerce is changing people's daily life and their shopping habitations.

Acknowledgements:

Most thanks go to my wife Bo whose supporting, encouragement, and understanding make my dream comes to true. I also thanks to my parents for their patience because it took me so long to work on my thesis. I take this opportunity to express my gratitude to my advisor Professor Peter A. Ng whose encouragement, supporting, enthusiasm, and knowledge are so important to me on this work. Special thanks go to Professor Bing Chen and Professor Alexander D. Stoyen for spending lot of time to review my thesis. Finally, I would like to thank all my friends, department and university staffs who give me all helps whenever I need it.

TABLE OF CONTENTS

ABSTRACT.....	i
ACKNOELEDGEMENTS.....	iii
LIST OF TABLES.....	vi
LIST OF FIGURES.....	vii
CHAPTER I: Introduction.....	1
CHAPTER II: Developing Technology Strategy for Online Business.....	7
Marketing Strategies on the Internet.....	7
Basic Online Architecture.....	9
Software Standards and Languages.....	10
Integration with Application Tools.....	13
CHAPTER III: Some of The Electronic Commerce Related Issues.....	16
Opportunities and Benefits of Electronic/Web Commerce.....	16
Three “Audiences” for Electronic Commerce.....	20
Business-to-Business (B2B) Networking.....	21
Business-to-Consumer Linkages.....	22
Business Intranets (Peers).....	23
B2B vs. B2C.....	24
International Agreements of Electronic Commerce.....	27
Online Marketing Size Assessment.....	29
CHAPTER IV: Online Security.....	32
Security on the Internet.....	32
Web Secure Protocols (Transport Protocol) for Electronic Commerce.....	37
Secure Sockets Layer (SSL).....	38
Secure HyperText Transfer Protocol (S-HTTP).....	39
Secure Electronic Payment Protocol (SEPP).....	41
SEPP Process.....	42
Secure Electronic Transaction (SET).....	44
Cryptography.....	47
An Overview of Cryptography.....	47
Some Basic Elements of Cryptography.....	48
RSA: The Keeper of the Algorithm.....	50

Private Key Cryptography vs. Public Key Cryptography.....	50
A Simple Example.....	52
CHAPTER V: On-line Shopping Solutions.....	56
IBM Net.Commerce (WebSphere Commerce Suite).....	57
HP Emporium.....	69
BroadVision One-to-One Commerce.....	70
Microsoft Commerce Server.....	71
Open Market LiveCommerce.....	72
Yahoo Store.....	73
Intershop Online.....	73
EIMedia NetSell.....	74
Basic features of an e-commerce application.....	74
CHAPTER VI: The Future of “Cyber Market”.....	76
CHAPTER VII: Conclusions.....	81
GLOSSARY.....	86
REFERENCES.....	89

LIST OF TABLES

Table 1-1. Current available types of Internet connections and their speeds	3
Table 3-1. Differences between business and consumer characteristics for electronic commerce.....	25
Table 3-2. A do-it-yourself exercise to estimate the size of Internet commerce.....	31
Table 5-1. Basic components of an E-commerce application.....	75

LIST OF FIGURES

Figure 1-1. Internet access at 2000 by different regions of the world	5
Figure 2-1. Basic components of a simple online business site.....	10
Figure 3-1. Internet commerce is about the convergence of the Web with traditional electronic commerce.....	20
Figure 3-2. Business customers and consumers represent different segments of Internet commerce.....	24
Figure 3-3. Global online users by various regions at 2005.....	26
Figure 4-1. The steps of a SET purchase using public-key cryptography.....	45
Figure 5-1. Target online shop homepage.....	59
Figure 5-2. Saks Fifth Avenue homepage.....	61
Figure 5-3. Shop Our Catalogs.....	62
Figure 5-4. Shows the available products.....	63
Figure 5-5. Shows one of the product customer selected.....	64
Figure 5-6. Shopping Bag (Traditional Shopping Cart).....	65
Figure 5-7. Shows checkout steps.....	66
Figure 5-8. Shipping information input fields.....	67

2. Basic Online Architecture

The basic architecture of online business systems consists of a number of distinct components, operating in a reliable and secure manner. Figure 2-1 [17] illustrates the basic components of a simple online business site. Online business sites are feature-rich and have become more functionally complex. Traffic between these sites (such as the total number of their customers who have visited these sites, and the total number of purchase order being submitted) will be increased exponentially. As a result, the simple Web server architecture has expanded rapidly into tiers of applications and database servers. This expanded architecture allows high-performance online business sites to achieve greater scalability and flexibility.

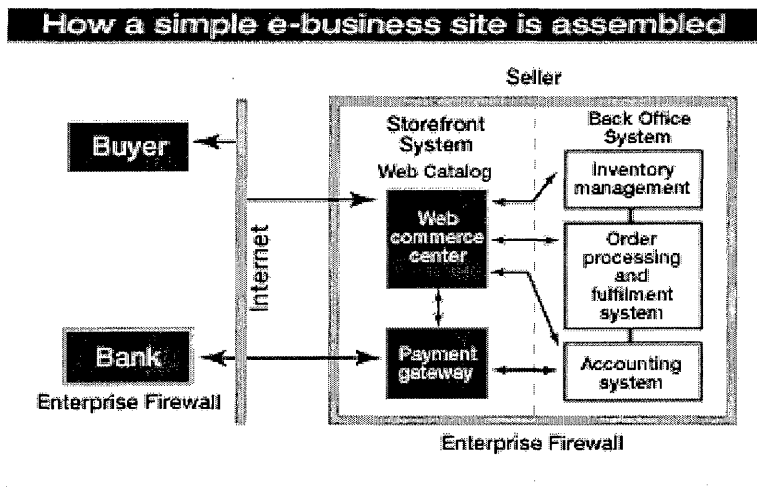


Figure 2-1. Basic components of a simple online business site

As Internet architecture has become more and more advanced and secure, the hardware components required to interface with the Web from both client and server perspective have increased in number and sophistication.

The benefits of Internet software standards go beyond their use on the public Internet. Within an organization, individual pieces of various hardware components are normally connected to each other by a hard-wired network to form a local area network (LAN), which is inaccessible from its outside. They may still, however, benefit from sharing information in the HTML or XML formats designed for the Internet. This application of information sharing on an internal within this private local area network is referred to as an intranet.

Similarly, for communicating securely with their business partners, many organizations currently use the infrastructure of the Internet, and yet reserve the availability of some of the channels away from the general public. This controlled and limited access to information through the wide area network (WAN) creates an extranet.

3. Software Standards and Languages

Information can be stored in a rigorous format as data. Sharing information could be done easily by standardizing the data format among various systems. Therefore, standardization of data, which becomes the heart of Web commerce, is the primary

reason that the Web is available to so many people throughout the whole world. By means of software standards and commonly used scripts and programming languages, text and data can be exchanged between any given Web site at a Web server and any registered Web user (or called a Web client), who connects their computer on the Internet from any corner of the world. In the following, we shall discuss some of the major software standards and languages that ensure that Web users can get the same and consistent messages.

HTML (HyperText Markup Language). The HTTP protocol defines how the messages can be exchanged between a Web server and a Web client. HTML is a document description language that consists of text and fixed tags. Tags describe the attributes of the text and other contents and are used by clients to determine how to display the text on the screen or perform other manipulations.

Each version of HTML has added new tags, which then must be implemented by all clients. A tag begins with an “<” symbol and ends with an “>” symbol. For example, the symbol <TABLE> is used to begin to insert a table and the table is ended by following the symbol </TABLE>. Any plain text can be begun after introducing a symbol and the text is ended by following the symbol .

XML (eXtensible Markup Language). XML is a specification for generating new languages that allows easy identification of data types in multiple formats, whereas

interpreted languages for the Internet are Java*, JavaScript*, and VBScript*, which resembles Visual Basic.

These languages are designed to be platform-independent (any operate system) and can be processed by any Web browsers (Internet Explore, Netscape Navigator, or AOL) running on any client operating systems as long as the browsers can understand these languages.

4. Integration with Application Tools

Once equipped with the necessary hardware, software and application tools to establish a Web presence, the business must then address various issues of integration with its systems before it can effectively conduct business over the Internet. Integration is critical to electronic business. It bridges the connection of an organization's electronic business systems and its pre-existing enterprise applications. This section focuses on the near-term technologies to be used by organizations, as they begin to integrate existing information technologies with new electronic business systems.

There are several approaches to integrating the existing information technologies with new electronic business systems. Their applicability depends on the extent to which an organization uses electronic business. These approaches can be loosely grouped into four

speed, making a connection and accessing to the Internet only for around \$300 per month. For most cases, this is cheaper than the rental of a business area that its owner would have to pay for physical real estate, and, has to pay any other expense in the same time during the rental period.

Some of the opportunities and benefits of electronic commerce [5] are as follows:

- Reduced costs to buyers from increased competition in procurement, as more suppliers are able to compete in an electronically open marketplace. Companies that sell their products through traditional catalogs and 1-800 numbers can expand their ability to reach additional global customers at a low marginal cost.
- Reduced costs and increased efficiency to suppliers by electronically accessing on-line database of bidding opportunities, by creating on-line ability to submit bids, and by allowing on-line review of awards.
- Reduced time, errors, and overhead costs in information processing by eliminating requirements for re-entering data.
- Reduced costs to inventories, as products supply and services providers are always electronically connected through just-in-time-inventory and integrated manufacturing techniques.
- Increased access to real-time inventory information, allowing to process rapidly any orders, with reduced costs due to discard of huge paperwork.
- Reduced total business transactions' time to be completed, especially the payment transaction time.

- Enhanced quality of products taking advantage of standardizing specifications and increased competitive sales by allowing to expand easily its markets and creating the ability to produce customized products.
- Created new markets by providing ability for reaching its potential customers in an easy and less expensive manner.
- Easier entry into new markets as the market becomes more even between companies of different sizes and locations.
- Faster time to market as business processes are linked, eliminating time delays between steps and the engineering of each sub-process within the whole process.
- Electronic commerce created new business opportunities in which businesses and entrepreneurs are continuously on the lookout for new and innovative ideas as viable commercial ventures.
- Optimization of resource selection as business build cooperative teams to work opportunities to increase chances of success, and to give the customer a mix of capabilities more precisely meeting the customer's requirements.
- Increased access to a client base by identifying and locating new clients and new markets.
- Improved product analysis as businesses are able to perform product analyses and comparisons and report their findings on the Internet.
- Improved market analysis as the large and increasing base of Internet users can be targeted for the distribution of surveys for an analysis of the marketability of a new product or service idea. Surveys can reach many people with minimal effort on the part of

the surveyors. Once a product is already marketed, businesses can examine the level of customer satisfaction.

- Businesses can access information from any countries around the world as long as the remote computer systems are connected on the Internet. It is faster than transmissions via fax or transfers via mail services or even special services.
- Information distribution is easy and fast since businesses can place documents on servers on the Internet and make them accessible to millions of users. Creating Web documents and Web sites improves the availability of the documents to a client base larger than the circulation of many major newspapers.
- Transferring on-line documents over the Internet takes a short period of time compare sending by the regular or express mail services, and it makes the documents transfer cost-effective because this can save money on those services. Most, if not all, Internet access providers do not charge by the raw number of bytes transferred across their networks, unlike some of other commercial information services.

“The promises of electronic commerce are pretty heady,” said Karen Whilt [1], who is the senior vice president of worldwide marketing and business development at Oracle Corporation. “We are going to minimize transaction costs, reduce cost structures, maximize production quality, reduce time-to-market and open new markets, and somehow, through all this, gain competitive advantage.” From his conclusion, the benefits of electronic commerce can be seen very clear.

Since the electronic commerce creates lots of opportunities and has lots of benefits for both businesses and consumers, it is significant that the investment community, once skeptical or indifferent, is also beginning to see the economic potential of the Internet. In August 1997, investment-banking firm Goldman Sachs [1] concluded that “cyber commerce” over the next decade “will create hundreds of billions of dollars of new Internet-driven market capitalization across many industries, much like the PC industry over the previous decade.

2. Three “Audiences” for Electronic Commerce

At its early stage in the Internet’s evolution, one of the most difficult challenges is conceptualizing a new taxonomy for electronic commerce. One of the most useful categories for understanding the medium’s potential is its distinct “audiences (sectors)”.

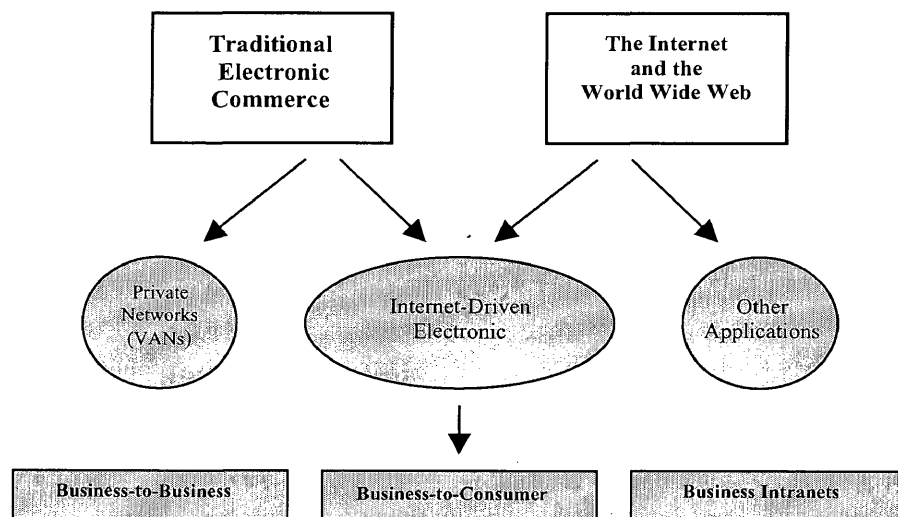


Figure 3-1. Internet commerce is about the convergence of the Web with traditional electronic commerce.

Over time, the introduction of Intranets brought some alterations on social relationships within a company and thus its management style and values. Intranet-driven organizations tend to eliminate their hierarchy and their structures become much flattened. Employees are given greater autonomy and responsibility, making their independent knowledge and creativity to be an important company asset. For the organization with Intranets facility, decision-making can occur quicker than in conventional organizations, based on greater supplies of timely information.

d) B2B vs. B2C

It is very easy to see that what are their service objects from the characters “B” and “C”. The B2B market relates to: (1) businesses selling products or services to one another, with a given organization serving as either buyer or seller, or (2) transactions and information relating to back-end processes between suppliers, partners, or channels, such

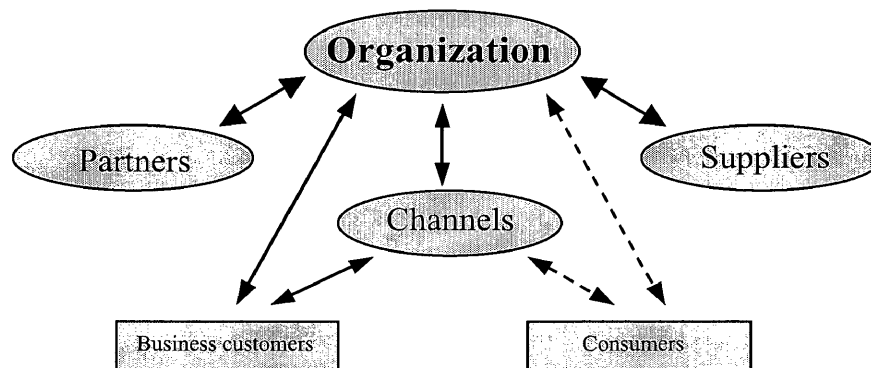


Figure 3-2. Business customers and consumers represent different segments of Internet commerce

as ordering, paying, EDI, basic and advanced procurement services, distribution support, and logistics management. The B2C market focuses on the consumer as the end user or buyer (Figure 3-2). For businesses, the term buying means procurement, whereas for consumers, it simply means shopping.

Table 3-1. Differences between business and consumer characteristics for electronic commerce

CHARACTERISTIC	BUSINESS	CONSUMER
Percentage on-line	High	Low
Total potential value of transaction	High	Medium
Value/price sensitivity	Low	High
Know relationship	High	Low
Number of customers	Low	High
Time required to “get in or out” of relationship	Long	Short
Motivation to improve efficiency of transactions	High	Low

The differences between B2B and B2C electronic commerce (Table 3-1) suggest that the B2B sector will develop more rapidly, because a higher percentage of businesses is connected to the Internet. Companies are organized to improve operational efficiencies and to integrate supply chains. Centralized decision-making and CEO leadership can also bring swift changes. However, the speed at which consumers begin to adopt certain technologies at slower, more predictable rates, regardless of a given technology’s benefits

is not to be underestimated, especially when contrasted with the relative shortage of B2B Internet applications.

Over the long term, consumers are expected to embrace many conveniences, cost savings, personalization, and other features of online shopping. As this market is growing, online shopping will provoke far-reaching changes in the global's retail businesses and in people's daily buying habits.

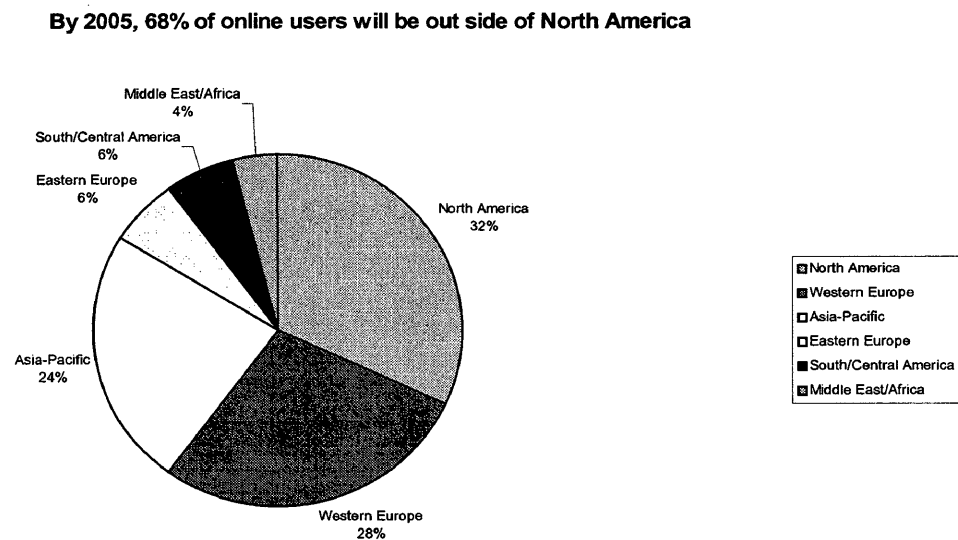


Figure 3-3. Global online users by various regions at 2005

should be \$0.6 billion in 2000 and \$1.5 billion in 2003. If you live in a country where the Internet is not well developed, you can apply different ratios to the number of people who might buy over the Internet, or to the average amounts they represent. But you have to start by knowing approximately the total number of Internet users.

Let us assume in Table 3-2 that you are interested in particular segment of the industry—for example, flowers. We will use the following fictitious for 2000 as our assumptions, based on the Canadian data. If approximately 3 percent of all Internet users (5,000,000 multiplied by 3% = 150,000 people) spend an average of \$60 per year on flowers, the total size of that segment is \$9 million (150,000 multiplied by \$60 = \$9,000,000).

How is the other major market—B2B? It is generally accepted and assumed that the size of the B2B market is about 7 to 10 times of that the size of the B2C market. This consists of all B2B applications, including the value of both products and services exchanged during business processes among organizations. Base on the above approach and the estimated values from the B2C market, it gives Canada \$ 6 billion for 2000 and \$28 billion for 2003 from B2B market.

From the above simple estimation and calculation, the market size is very clear for both B2B and B2C. According to the example, you can choose the industry that it will catch

your interest and use the method to estimate by yourself. The next step is the decision making.

Table 3-2. A do-it-yourself exercise to estimate the size of Internet commerce

PARAMETER	2000	2003
Number of users over the age of 16 on the Internet	5 million	8 million
Percentage of those who buy on the Internet	40%	70%
Total eligible buyers	2 million	5.6 million
Average buying value per year	\$300	\$500
Total value purchased over the Internet	\$0.6 billion	\$2.8 billion

IV. Online Security

1. Security on the Internet

As business activities grow on the Internet, security is becoming a very critical and important issue to address. We need to take security of any processes on Internet into account if we want to address the stakeholders' satisfaction. As a matter of fact, the dominant issue of any business transactions in electronic commerce today is security. Security relates to three general areas: secure file/information transfers; secure transactions; secure enterprise networks, when used to support Web commerce. Many of their observers and proponents advocate strongly that the security issue must be addressed quickly in order for companies to start investing in electronic commerce. There are indications that merchants are taking a wait-and-see attitude in electronic commerce on the Internet. Until there is a dominant standard or there is universal software that will support a variety of encryption and transaction schemes that they feel good about it. The market is looking for a comprehensive solution (in a software product) that the merchants and banks can use to support all demand functions on their Web business.

Online security has several fundamental goals [5]:

1. **Privacy:** The privacy of documents and personal information could be supported by password usage, encryption, and access-control systems.

2. Integrity: All data and applications should be safe from modification without the owner's consent.
3. Content integrity: The ability for identifying any modification made to the covered information.
4. Authentication: The assurance of the computer users who are the authorized users of that system could be provided by frequent check of their password or ID or any other verification information.
5. Availability: The end system (host) and data should be available when needed by the authorized user from anywhere on the Internet.
6. Signature: The ability for specifically identifying the entity associated with the information from person to person.
7. Non-repudiation of origin: The ability for identifying the initial/original sender of information versus the intermediary senders.
8. Non-repudiation of receipt: The ability for identifying that the information was received by the desired destination on the Internet in a manner that cannot be repudiated. The information has been opened and interpreted to a certain degree.
9. Non-repudiation of delivery: The ability for identifying whether the information was delivered to an appropriate intermediary recipient in a manner if cannot repudiate. Another issue that should be managed is just plain fraud, that is, the buyer simply provides out-of-date or incorrect credit card information.

Web-based commerce is beginning to penetrate the market, but security becomes a critical issue for its further penetration. For instance, the Cisco Connection Online, which is considered to be an effective Web commerce site, runs on Netscape Secure Commerce Servers. A firewall is used to screen out unregistered customers (All the regular customers are considered to register before they can use that online site.).

Registration's tools help manage electronic commerce on the customer side. At registration, a customer submits purchasing authorized information. When a customer configures a product, the request can automatically be sent to the next person in the purchasing chain for pricing or approval. Within an hour, the customer can use a status agent to check on the order and see when the product is scheduled to ship. But for pervasive penetration, security is indispensable. By far, the least expensive approach to handling payments over the Internet is to select a toolkit that has a credit card authorization capability.

Security concerns apply to both the network transport portion and the host portion of the end-to-end infrastructure. The conventional concern is that the problem is in the network transport. Because information flows through the Internet in a store-and-forward fashion over shared computers (nodes), it is, in fact, susceptible to security attacks. The TCP/IP packets flow through many different nodes (routers) on the way to their final destination specified by the URL (Uniform Resource Locator). Any of these intermediary nodes can in principle be the source of a security breach either by those having physical access to

these devices or by hackers that log in into the administrative side of the node and possibly re-route a trap or a data flow. This can cause concerns for both businesses and their customers. However, in routers, data is only stored for a very short transition time. Furthermore, routes are updated dynamically, so a hacker-defined route could be quickly eliminated by device. Some people hold the opinion that security infractions are more likely at the host/server level. "Corrupting the data while in transit is like shooting a moving target; it is easier to shoot a stationary target, where data sitting in an Internet-connected server." [6]

Consider an example. In the WWW environment, both Java and the Common Gateway Interface (CGI) can become host-security problems. With Java, applets can be downloaded into the client side of a Web setup. Applets are programs that execute locally on the user's machine and can, in principle, perform negative functions. In addition to taking on virus like forms (e.g., reformatting the driver or erasing files), they could be programmed to contact a hacker's system and send a copy of the user's own password/profile file. CGI programs run on the WWW server in response to client requests. CGI programs perform general computational functions including accepting form data, communicating with other computers, and creating dynamic pages. On the negative side, CGI programs could be manipulated to create havoc or transmit out files containing credit information.

All of the businesses with servers containing confidential data connected to the Internet do not want the public to have unauthorized access and view to these files. But, at the same time, they might want the public to have access and view to specific parts of their information base for doing the business with the public.

Any services of businesses, that require payment over the Internet by methods including credit card transactions also need to be cautious: if there transactions are not secured, or if any hackers could access (steal and then sell) the customers' account information.

Enterprise network access security is addressed using firewall and bastion in the enterprise network or even simply using a stand-alone public access host. There is a desire to protect data between two sites using the Internet as a transport (a concept called virtual private network, VPN). This can be easily accomplished by having all data between the two enterprise network firewalls encrypted and then all data transmitted between VPN and public access host of enterprise network. Encryption mechanisms are now found in commercial firewall software, such as Milkyway Networks Corporation's Black Hole and Trusted Information Systems' Gauntlet.

Uncertainty as related to security can discourage potential customers from using the Internet as a source of commerce for potential Web business providers. VANs (Value-added Network) have been using fears over Internet security as a marketing argument to help sell their own services, which are perceived to be more secure. It is true that the

Internet currently does not provide network security by itself. But the technology for solving the problem has been available for decades and the price for proving the Internet with security has reduced significantly. A good solution for securing the information in Internet is simply for the client and the server to encrypt the appropriate information using public-key encryption methods before the information is transmitted. For any large file or any application having to transmit information at DS1 or DS3 rates, an accelerator board to support encryption or even a stand-alone adjunct processor may need to be used. But for smaller files and/or data transferred at dial-up speeds, the processing power of the access device should be adequate to support software-based encryption.

The use of public-key encryption has confidence to solve much of the Internet security problem. Two-key encryption (with one public key and one private key) is already being made standard on the Netscape commercial servers and results in the ability to send confidential information such as credit card number through the Internet.

2. Web Secure Protocols (Transport Protocol) for Electronic Commerce

The hypertext transfer protocol (HTTP), which forms the basis of the Web, offers no inherent security for transmission of data across the Internet. There are two protocols provide the abilities and can get around these problems: SSL (Secure Sockets Layer) and S-HTTP (Secure HyperText Transfer Protocol). Both of them provide the foundation for using encryption to protect confidential information to be secure when it was transferred

through the Internet. The other protocol that is commonly used is the Secure Electronic Payment Protocol (SEPP) and we will address it.

a) Secure Sockets Layer (SSL)

The Secure sockets layer (SSL) protocol, which is developed by Netscape Communications, is a security protocol that provides protection of privacy over the Internet. The protocol allows client/server applications to communicate over the Internet that data transmissions cannot be altered or disclosed by third-party. Servers are always authenticated and clients are optionally authenticated. The technology supports for key exchange algorithms and hardware tokens. The strength of SSL is that it is application-independent. HTTP (HyperText Transfer Protocol), Telnet, and FTP (File Transfer Protocol) can be placed on top of SSL transparently. SSL provides channel security through encryption and reliability through a message integrity check.

SSL uses a three-part process to finish its procedure. First, information is encrypted to prevent unauthorized disclosure. Second, the information is authenticated to make sure that the information is being sent and received by the correct party or its correct destination. Finally, SSL provides message integrity to prevent the information from being altered during interchanges between the source and sink. SSL depends on RSA [10] (A public-key encryption algorithm based on exponentiation in modular arithmetic and is invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It is the only

algorithm generally accepted as practical and secure for public-key encryption.) it would to encrypt for exchange of the session key and client/server authentication and for various other cryptographic algorithms.

When a customer submits a request to purchase merchandise over the Internet, the online company responds with public key that the customer's computer use it to encrypt sensitive information as he/she will send it back to the online company. This sensitive information is sent back to the company, and in turn the company uses a private key (only holding by the online company itself) to decrypt the information. The process is transparent to customers, and hence it is easy to use. The shoppers then enter their credit card numbers. The SSL encrypts them and sends the encrypted files to the merchant. The transmission proceeds as soon as SSL decrypts the files.

b) Secure HyperText Transfer Protocol (S-HTTP)

The Secure HyperText Transfer Protocol (S-HTTP) is a secure extension of HTTP developed by Enterprise Integration Technology the Commerce.Net Consortium. S-HTTP offers security techniques and encryption with RSA [10] method and provides the ability for both servers and clients to send encrypted information, along with other payment protocols. As an application protocol, S-HTTP can be only used for HTTP transactions.

For secure transport, S-HTTP supports end-to-end secure transactions by incorporating cryptographic enhancements to be used for data transfer at the application level. This is in contrast to existing HTTP authorization mechanism, which requires the client to attempt access and be denied before the security mechanism is employed. S-HTTP incorporates public-key cryptography from RSA Data Security in addition to supporting traditional shared secret password and Kerberos-based security system. One of the more important features is that it does not require the client to use a public key.

S-HTTP supports three types of protection: encryption, authentication, and signature. The RSA Data Security ciphers used by S-HTTP utilize two keys: files encrypted by one key (normally called public key) can only be decrypted by application of the other key (normally called private key). A company generates a pair of these keys, published one and retains the other. When any another company wishes to send a file to the first company who holds the unpublished key, it encrypts the file with the published key of the intended recipient. The recipient decrypts it with the private key. S-HTTP allows Internet users to access a merchant's Web site and supply their credit card numbers to their Web browsers. It encrypts the card number, and the encrypted files are then sent to the merchant. Then, S-HTTP decrypts the files and relays back to the users' browsers to authenticate the shoppers' digital signatures. The transaction proceeds as soon as the signatures are verified.

c) Secure Electronic Payment Protocol (SEPP)

IBM, Netscape, GTE, CyberCash, and MasterCard have cooperatively developed SEPP (Secure Electronic Payment Protocol), which is an open, vendor-neutral, nonproprietary, license-free specification for securing on-line transactions. Many of its concepts were rolled into SET (Secure Electronic Transaction), which is expected to become the de facto standard.

SEPP addresses several major business requirements:

1. To enable confidentiality of credit card information
2. To ensure integrity of all payment data transmitted
3. To provide authentication that a cardholder is the legitimate owner of a card account
4. To provide authentication that a merchant can accept MasterCard branded card payments with an acquiring member financial institution

SEPP is equivalent to an electronic paper charge slip with signature and submission process. It takes an input from the negotiation process (amount of payment, order descriptions, payment method, etc.) and causes the payment to happen via a three-way communication among the cardholder, merchant, and acquirer (financial institution).

SEPP only addresses the payment process without addressing the privacy of non-financial data. Hence, it is suggested that all SEPP communication be protected with

encryption at a lower layer, such as with Netscape's SSL. Negotiation and delivery are also left to other protocols.

d) SEPP Process

SEPP assumes that the cardholder (consumer) and merchant (business provider) have been communicating in order to negotiate terms of a purchase and generate an order. These processes may be conducted via a WWW browser. Alternatively, this operation may be performed through the use of traditional electronic mail. The SEPP system is composed of a collection of elements involved in electronic commerce. There are as follows:

- **Cardholder.** This is an authorized holder of a bankcard supported by an issuer and registered to perform electronic commerce.
- **Merchant.** This is a merchant of products , services, and/or e-products who accepts payment for them electronically and may provide selling services and/or electronic delivery of items for sale.
- **Acquirer.** This is a financial institution that supports merchants by providing service for processing credit-card-based transactions.
- **Certificate management system.** This is an agent of one or more bankcard associations that provides for the creation and distribution of electronic certificates for merchants, acquirers, and cardholders.

- Banknet. This represents the existing network, which interfaces acquirers, merchants , and the certificate management systems.

These elements for Web commerce do exist today and interact through existing mechanisms, with the exception of the certificate management systems. Several basic transaction messages are required in a SEPP-based environment. When variations of the standard flow occur, additional data will be required in the supplementary messages.

Messages for SEPP-compliant processing of payment transactions include:

- Purchase Order Request
- Authorization Request
- Authorization Response
- Purchase Order Inquiry
- Purchase Order Inquiry Response

Additional messages for on-line customer are:

- Initiate
- Invoice
- Purchase Order Response (with Purchase Order Status)

Message for off-line (i.e., e-mail) transactions or transactions sent to merchant not on-line with the acquirer

- Purchase Order Response (acknowledgment without authorization).

The simplified SEPP processing form occurs as follows. The buying cardholder begins the transaction by sending the merchant an *Initiate* message. The merchant responds with an *Invoice* message containing information used by the buying cardholder to validate the goods and service and the transaction information. The buying cardholder then prepares a *Purchase Order Request* that contains goods and service order validation information and the buying cardholder's payment and personal information which are encrypted in a manner so as to only be decrypted by the acquirer. The merchant receives the *Purchase Order Request*, defines a format of an *Authorization Request*, and sends it to the acquirer. The *Authorization Request* contains the confidential cardholder's payment instructions. The acquirer processes the *Authorization Request*. The acquirer then responds to the merchant with an *Authorization Response*. The merchant will respond to the buying cardholder with a *Purchase Order Response* if the *Purchase Order Response* message was not previously sent. At a later time, the buying cardholder may initiate a *Purchase Order Inquiry* to which the merchant will respond with a *Purchase Order Inquiry* response.

3. Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is an open specification developed jointly by Visa and MasterCard: the future for on-line payments, specifically and cooperatively developed to protect buyers and sellers in conducting "card-not-present" transactions over the Internet. SET is becoming the de facto standard for on-line transaction security

and the industry is counting on SET to accelerate Internet electronic commerce. It relies on digital certificates issued to consumers; the certificates contain credit card information that is verified by credit card issues through a certification authority. Several key functions of the specification are listed as follows and its operations are shown in Figure 4-1.

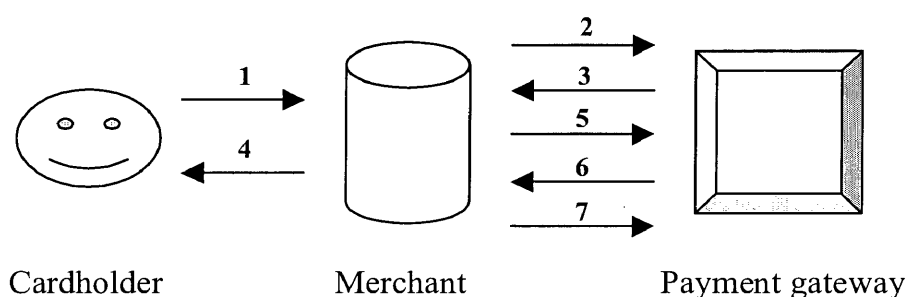


Figure 4-1. The steps of a SET purchase using public-key cryptography: (1) Cardholder requests purchase; (2) Merchant contacts payment gateway for authorization; (3) Payment is authorized; (4) Cardholder is notified of authorization; (5) Merchant requests payment capture from gateway; (6) Token is issued to merchant; and (7) Merchant redeems token for transfer into its bank account.

- Provide for confidential payment information and enable confidentiality of order information that is transmitted with payment information
- Ensure integrity for all transmitted data
- Provide authentication that buyer is a legitimate user of a branded bankcard account
- Provide authentication that a merchant can accept bank card payments through its relationship with an appropriate financial institution
- Ensure the use of the best security practices and design techniques to protect all legitimate parties in an electronic commerce transaction

- Ensure the creation of a protocol that is neither dependent on transport security mechanisms nor prevents their use
- Promote and encourage interoperability across software and network providers

Let consider the role of the SET [6] in on-line shopping and payment processing. An e-shopping consists of eight phases. Out of the eight defined phases of e-shopping in the following list, SET is active in phases 4, 5, 6, and 8.

Phase 1. Cardholder (customer) browses for items via the Internet based Web.

Phase 2. Cardholder selects necessary items from the above resource for purchase.

Phase 3. Cardholder completes an order form, including total costs, shipping, handling, and taxes (Web shopping not always need to pay the tax).

Phase 4. Cardholder selects the form of payment card to use for the order. SET is initiated at this point.

Phase 5. Cardholder sends completed order form and payment instructions to the Merchant. SET is used to sign these order forms and payment instructions digitally using the Cardholder's digital certificate to prove they came from the Cardholder and no one else.

Phase 6. Merchant requests payment authorization from the Issuer of the payment card using its Merchant account through its Acquirer's payment system. SET wraps these messages in cryptography to assure their privacy and confidentiality over the Internet during their transmission.

Phase 7. Merchant ships goods or performs requested services based on the order.

Phase 8. Merchant requests to capture the payment that was previously approved for processing in phase 6.

SET wraps these messages in cryptography, to ensure their privacy and confidentiality that could not be reached by any other parties or individuals. Those phases, which are not actively involved by SET are considered out of scope activities, and their implementation is left up to the involved parties. In addition, those interfaces to systems required for using SET are also out of scope to the specification. SET provides open and robust data structures and corresponding security to handle any type of order processing. It establishes an infrastructure for banks and Merchants to plug into using software they customize to meet infrastructure requirements.

4. Cryptography

a) An Overview of Cryptography

SET's features are implemented using the application of cryptography [6]– the science of secret writing. Cryptography enables the storage of information in certain forms that are revealed only to those permitted users and are hidden from everyone else. In the 20th century, the cryptography technique is begun to use by the government to protect their private and sensitive information and for communication purposes. In the last 25 years,

the government and military organizations were the exclusive users of cryptography to secure their own sensitive and private data and to try and crack everyone else's.

Since the 1970s, academic researchers' interest in cryptography has grown at a tremendous rate. With the researchers' proposal, public have gained access to various cryptography techniques permitting personal information protection and enabling the conduct of secure electronic transactions. With the aid of supercomputers, massively parallel processors, various groups of hackers work together to try and crack the strongest cryptosystems. With increasing sophistication of modern computer technology, cryptography stands to evolve into a set of highly reliable and well-established practices. SET uses multiple layers of cryptographic elements.

b) Some Basic Elements of Cryptography

Cryptographers rely on two basic methods of disguising messages: transposition, where letters are rearranged into a different order, and substitution, where letters replace by other letters. Plain text is the message that is passed through an encryption algorithm, or cipher, and becomes ciphered text. When the ciphered text is passed through a decryption algorithm, it becomes plain text again and can be read by any users.

A strong cryptosystem is considered strong only until it's been cracked. While that may sound like common sense, one can never prove that a cryptosystem is strong – one can

only ensure that certain properties are present within. Each defeat of an attempt for cracking a cryptosystem serves to strengthen the belief in its ability to be secured. Once that belief is proven to be unfounded, the cryptosystem collapses and no one relies on it anymore. All strong cryptosystems have similar characteristics. Their algorithms are made known to the public by posting them on online forums and public-accessible documents. The detailed algorithms are inaccessible and therefore without the key. The strength of a cryptosystem's algorithm rests in the keys used to encrypt and decrypt (the longer the key the better). The basic idea is to keep the keys in secret rather than keep the algorithm in secret. Because keys are typically created using strong cryptography algorithm, the likelihood of their discovery or breach, through any method other than theft, is nearly zero. Strong cryptosystems will produce ciphered text that always appears to be random to standard statistical tests. They also resist all known attacks on cryptosystems and have been brutally tested to ensure their integrity. Those cryptosystems that have not been subjected to brutal testing are considered suspect and could not be used.

When the same key is used to encrypt and decrypt messages, it's called symmetric key cryptography. When different keys are used to encrypt and decrypt messages, it is called asymmetric key cryptography. The Data Encryption Standard (DES) [8] uses the former technique, while RAS (named after its inventors – Rivest, Shamir, and Adelman) uses the latter technique. SET uses a combination of DES and RSA cryptography to implement privacy, security, and authentication services.

c) RSA: The Keeper of the Algorithm

RSA, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, was the first public-key algorithm to support both encryption and authentication. Public key algorithm uses a pair of keys—a public key and a private key to encrypt and decrypt messages. You share your public key with all the people living in the world who are using the Internet. That means, anyone can use your public key to encrypt its own data. When you receive the encrypted data, you use your private key to decrypt it. Your private key always remains secret and could not be shared with anyone else. When you would like to send confidential data to other people, you use their public keys to encrypt the data, and receivers use their private keys for decryption. RSA is the most popular public key algorithm and to be considered one of the strongest algorithms commonly used. The RSA algorithm is based on the idea that it is difficult to prime-factor a large number or break it down into its prime components. RSA's public and private keys are based on a pair of 100- to 200-digital prime numbers.

d) Private Key Cryptography vs. Public Key Cryptography

Private key cryptography works by allowing each party to know the same secret codes, or keys, for encrypting and decrypting information. The keys only can be viewed and kept in private. The most widely used form of private key cryptography is known as the DES and is used by financial institutions to transmit information. It only works as long as both

parties keep the key in confidential. Any compromise for the key's security makes the system easy to attack. Private key cryptography has been the basis of most encryption system throughout history.

Public key cryptograph is a newer form of cryptography. In this public key system, one key is used to encode information, which can only be unlocked by a second key. The first key is publicly distributed to anyone who wants to send encrypted information. The person receiving information keeps the second key in secret. Because the public key can be freely published, these two parties do not have to hide this exchange of keys and are able to set up secure communication in plain view. This provides a distinct advantage over a private key system.

Public key cryptography results from a mathematical theory that states that certain mathematical operations are more difficult than other. For example, it is very easy for a computer to multiply two large numbers together, but it is much harder to determine the factors for s large number. Consider the following problem: $x = 53 * 71$. It is quite easy to solve this problem. But it is difficult to solve the problem $x * y = 3763$, where x or y is not equal to 1. To solve this problem, people must try multiple values for both x and y until he or she found the answer. This operation takes considerably longer time comparing with a simple multiplication. When working with computers you must simply increase the size of the numbers to make the problem harder for the computer to solve. This one-way difficulty is exploited in public key cryptography to create what are in

V. On-line Shopping Solutions

-- The Applications of E-commerce

From the market you can find thousands and thousands of different online shopping solutions. In this these, it is impossible to describe every available solution in details. For implementing an online shop, how does a right item select from a group of available products is an important issue. There are three basic options allowing any designer of future online company to make a decision. Buy a ready-make solution (such as IBM WebSphere and Intershop), rent space at an e-hosting solution (such as Yahoo Stores and Escalate Direct) or build the system from scratch with components and parts exactly to your specifications (such as Microsoft's Site Server Commerce Edition and Macromedia's ColdFusion).

If the companies who have the budget and also they know how to install a complete solution on their own and how to maintain it, then the first option -- a ready-made solution is best option for them. This requires programming knowledge and HTML knowledge for setting up and maintaining the shop. The second option, namely, the Electronic hosting solution is perfect for the smaller companies, which do not have the budget to implement and maintain a complex shopping solution. They may rent an online shop from an available ISP (Internet Service Provider), which has paid for the software and hardware and has the infrastructure to operate the online shop. The companies only need provide the layout and the information of their products for the online shop. The

third option is a complex one. It divides into two sub-options. HP calls them “Chapter one” and “Chapter two”. “Chapter one” shops use available tools with necessary information for setting up online shops at the very beginning points. It is easier to create complex online sites if those available tools are used and only requires little appropriate programming knowledge. “Chapter two” shops do not require to use those tools from beginning points to set up online shops. Any source on the Internet of those tools can be used to import into a complex online shopping solution not the components from single or same vendor and with little programming knowledge.

In the sequel, we shall introduce some of the available shopping solutions.

1. IBM Net.Commerce (WebSphere Commerce Suite)

IBM Net.Commerce [3], which was developed by IBM and is called the WebSphere Commerce Suite [12][18] in later versions, is a complex shopping system with shopping basket and full search functionality. It gives you the power, flexibility and scalability to create an end-to-end hosted e-commerce service, in a quick, easy and affordable manner.

Net.Commerce can create attractive, high-performance Web sites. It is a most significantly solution for e-business (both business-to-business and business-to-consumer) that is dynamic, scalable, and secure. Using Net.Commerce, merchants can design all features of the virtual storefront to create a unique product presentation that

meets their business strategies. It can easily create Web pages that dynamically retrieve the most up-to-date product, pricing, and inventory availability information from connected database.

Net.Commerce provides a variety of tools for entering and managing the data related to the store, including products and prices, shipping information, taxes, and payment information. The predefined database schema can be extended to add new store functionality, such as special time-limited promotions. The purchasing process can be adapted to suit the business's patterns of interaction with shoppers and interface with their existing systems in the company and connect to trading partners.

The product has three different versions: the START version, which is good for the small-to-medium companies, the PRO version, which is suitable for larger online retailers, and the third one, which is special make for ISPs.

WebSphere Commerce Suite has several editions, namely, Star edition, PRO edition, MarketPlace edition, and Service edition. This product will help developers grasping the next-generation of e-commerce in the process of building their businesses on the Web, or expanding their businesses on the Web. Since the Web has no boundary, it supports global e-commerce. WebSphere Commerce Suite provides multicultural functionality to support unique geographic requirements (its perfect for language translation). It adapts to multiple taxation laws, fluctuating currency, and payment regulations. Enable your

merchandising and marketing managers to create, update and manage catalog data regardless of geographic location or cultural preference. It also supports the mobile commerce. This allows the developers to extend their online shops to wireless customers whether they are gaining access using cellular phones, PDAs (Personal Digital Assistant) or other handheld devices.



Figure 5-1. Target online shop homepage

The typical online shop with its homepage could be one such as the Target store as shown in Figure 5-1. The SHOP icon provides their customers with the facility for ordering goods from the site without paper catalog. MY ACCOUT icon allows the users to manage the existed account or new account very convenient. All the different sun-folders clear the products so that the users can search the need easily by selecting from each category such as Electronics, Heath and Beauty, and Music/Books.



Figure 5-2. Saks Fifth Avenue homepage

We select one of the online shops called the Saks Fifth Avenue, to be our example here. The reader could be a shopper and experienced the online shopping at the Saks Fifth Avenue online shop. Figure 5-2 is the homepage of the shop, which contains main information with whole shopping guide.

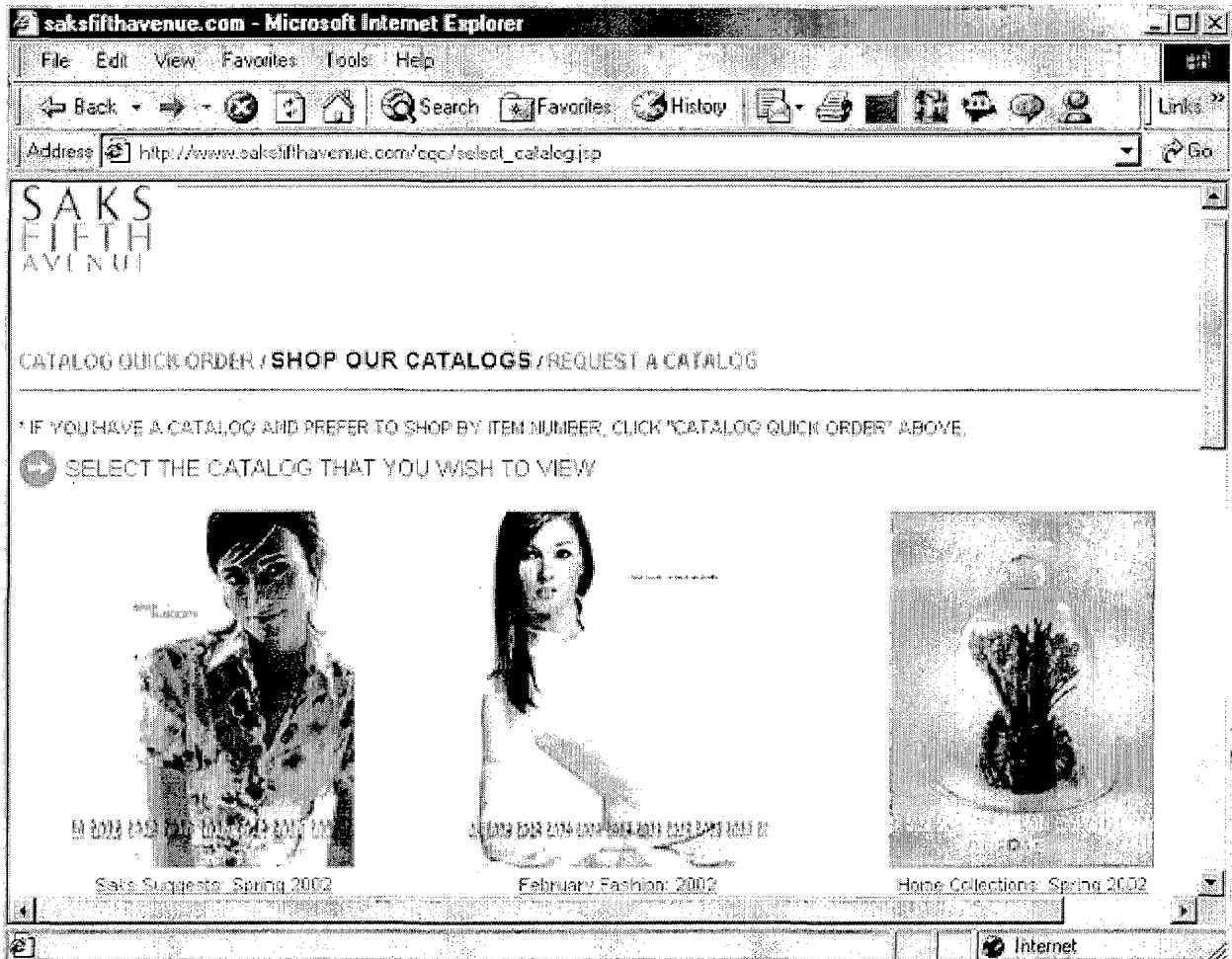


Figure 5-3. Shop Our Catalogs

Consider that the reader wants to buy some clothes from this online shop. We select CATALOGS/SHOP OUR CATALOGS. Figure 5-3 shows exact the same page as the reader clicks the right icons shows on Figure 5-2. Now it shows the easy read step on the window allowing the customers to follow the shopping instructions in ease. Then the reader selects the February Fashion 2002 catalog on Figure 5-3 for their purpose.

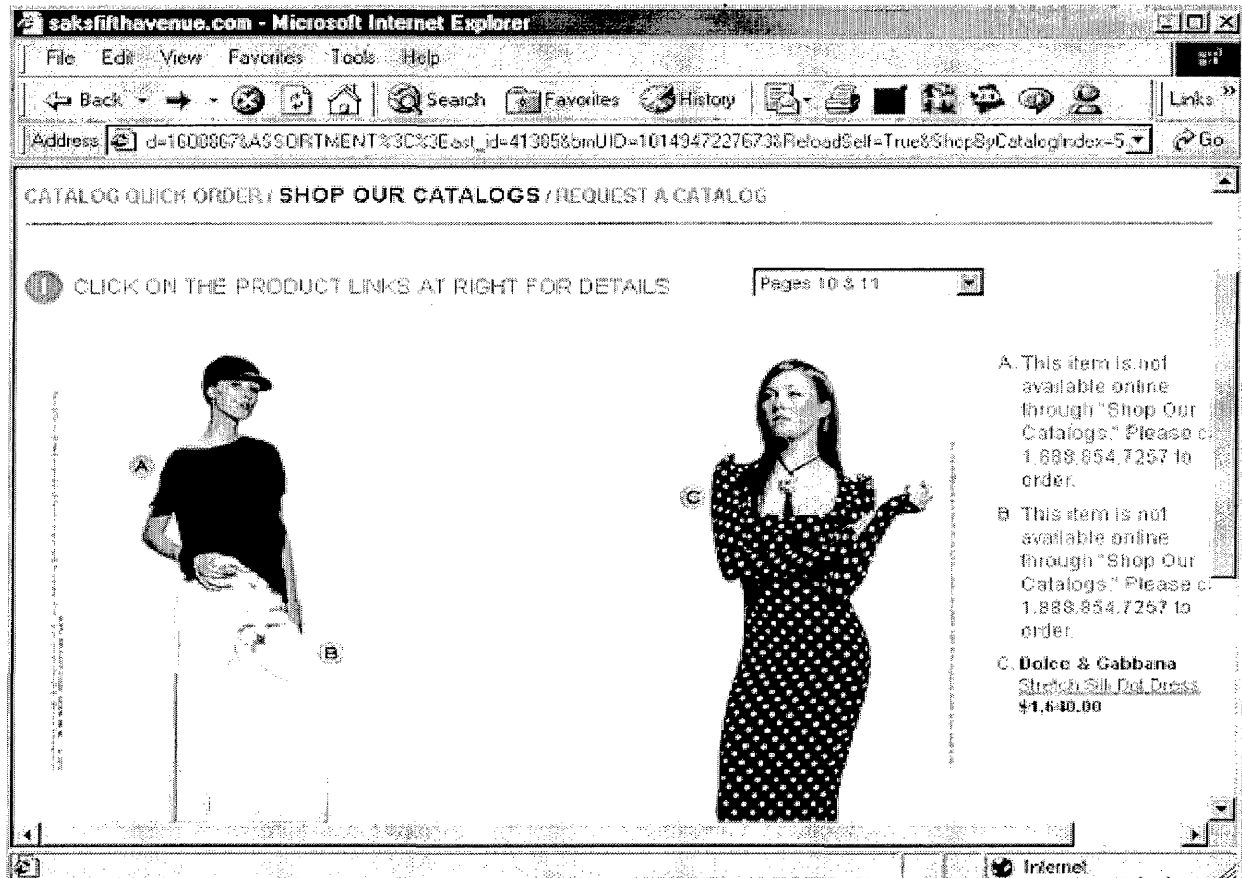


Figure 5-4. Shows the available products

Now the Figure 5-4 comes. As shown in this page, it has a pull-down list, which allows the customers to select all the available pages and view all the available products one by one. Each page shows what the products exact look like when they are dressed by the models. Pictures of models with different dresses are shown on the left side and the products' information is kept on the right side of the window. For instance, on this page items A and B are not available online but the order information from catalog is provided and item C has the product name, with its description of materials made and its price. Further detail information can obtain just clicking STRETCH SILK DOT DRESS.



Figure 5-5. Shows one of the product customer selected

After we select the item C from the previous page, the fourth window as shown in Figure 5-5 will be displayed. It contains several options for shoppers to select: MORE INFORMATION, VIEW THE LOOK, and CLICK TO ENLARGE IMAGE. For purchasing any of the items, a shopper can input the quantity as desire from QTY input field and the color and size can be chosen from the pull-down list as their prefer. ADD TO SAKS BAG push button is available on right side of the window for the shopper to complete the order.

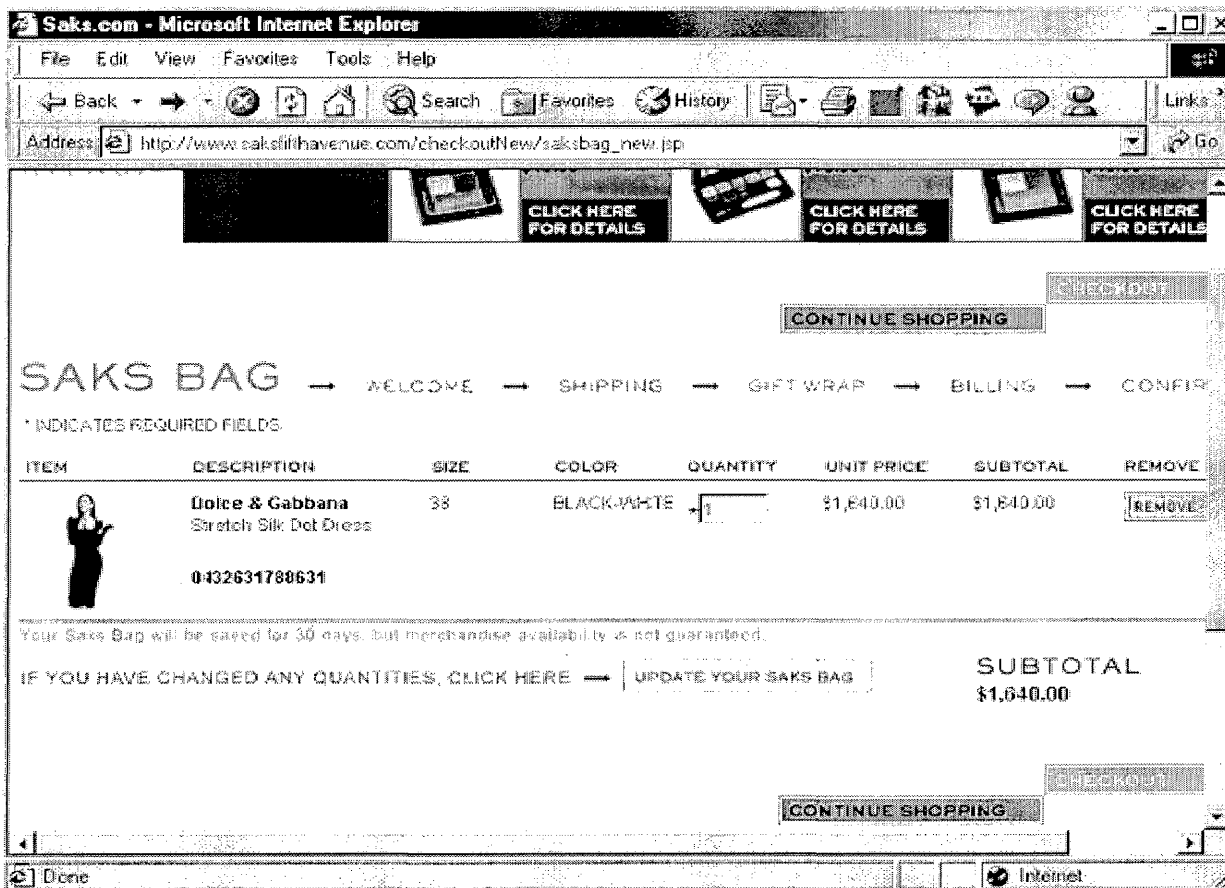


Figure 5-6. Shopping Bag (Traditional Shopping Cart)

As shown in Figure 5-6, this fifth window shows the detail of your shopping bag so far. If you decide to buy more items, you can push CONTINUE SHOPPING button; otherwise you can push CHECKOUT button for exit from the window. Other options such as UPDATE YOUR SAKS BAG and REMOVE buttons for their purposes.

Saks.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Links

Address http://www.saksifthavenue.com/checkoutNew/saksbag_new.jsp

SAKS FIFTH AVENUE

SAKS BAG — WELCOME — SHIPPING — GIFT WRAP — BILLING — CONFIRM

PLEASE SIGN IN SO WE CAN BETTER ASSIST YOU WITH YOUR SHOPPING EXPERIENCE

RETURNING CUSTOMERS PLEASE NOTE:
In order to make your shopping experience even easier, you no longer need to enter your "USER NAME" at saks.com. Simply enter your e-mail address and existing password to sign in.

* INDICATES REQUIRED FIELDS
E-MAIL ADDRESSES AND PASSWORDS ARE CASE SENSITIVE

PLEASE ENTER YOUR E-MAIL ADDRESS

I AM A NEW CUSTOMER
(YOU CAN CREATE A PASSWORD LATER)

I AM A RETURNING CUSTOMER AND MY PASSWORD IS:

FOR NEW PASSWORDS CLICK HERE

Done Internet

Figure 5-7. Shows Checkout Steps

Since the shopper decided to buy only that selected dress at this time, the CHECKOUT button was clicked. So the sixth window as shown in Figure 5-7 is displayed, and the first check out step is WELCOME followed by SHIPPING, GIFT WRAP, BILLING and COMFIRM. To be registered as a customer to buy the goods, you should give the specified required information of yourself that allowed to be verified later. The input fields allow the shopper to enter their information.

The screenshot shows a web browser window titled "Saks.com - Microsoft Internet Explorer". The address bar displays "https://www.saks Fifth Avenue.com/checkoutNew/welcome_new.jsp". The page content includes a navigation menu with links for "SAKS BAG", "WELCOME", "SHIPPING", "GIFT WRAP", "BILLING", and "CONFIRM". Below the menu, a heading reads "ENTER THE SHIPPING ADDRESS FOR THIS ORDER". A note states "* INDICATES REQUIRED FIELDS". The form contains the following fields:

- Title: A dropdown menu with "Select a Title" selected.
- First Name, MI, and Last Name: Three text input fields.
- Shipping Address: A multi-line text input field.
- City: A text input field.
- State: A dropdown menu with "Choose a state" selected.
- ZIP/Postal Code: A text input field.
- Country: A dropdown menu with "United States" selected.

 The browser's status bar at the bottom shows "Done" and "Internet".

Figure 5-8. Shipping information input fields

The SHIPPING step, as shown in Figure 5-8, allows the shopper to enter all the necessary information, including their shipping address for the vendor to ship their order whenever it is ready to deliver to the shopper in the next few business days depending on the shipping method the shopper was selected in this page.

The GIFT WRAP step gives the shopper an option if the shopper would like to vendor to be wrapped as a gift. In addition, the shopper can choose the wrap style, color, or any other options they provide here.

The BILLING step usually needs the shopper to provide the payment information authorized the online shop to charge the bill into the shopper's credit card account. This is the most secure step for all the online e-commerce, which is the major concern by most of them the shoppers. Because it contains all the private financial information of the shopper, who does not like share their information with others. We have addressed the security issue in previous chapter of this thesis.

The CONFIRMATION step confirms all the information that collects from pre-shopping. It should include the shopper's personal information (First Name, Last Name, E-mail Address, Mailing Address, Billing Address, Phone Number), product information (Quality, Quantity, Size, Color, Style), payment type (Amount, Credit Card Information) and this probable the last step before the shopper completes this shopping trip.

The leading online selling businesses and merchants on Internet include Amazon.com, Beyond.com, BUY.com, Nike.com and the most successful retailed department stores include Target, Staples, Compaq Computer, Saks Fifth Avenue, and Casual Corner all use IBM WebSphere Commerce Suite.

2. HP Emporium

HP Emporium [19] offers a cheap online shopping solution. The customers do not have to worry about the maintenance and operation for the first phase because it is totally managed and hosted by Hewlett-Packard. It allows companies to explore, evaluate and experience the full power of the online shop web for six months totally free of charge. With this solution, companies (usually they have insufficient money and knowledge in developing their online shop) are able to go online almost immediately with the chance to pick up the required knowledge in the meantime. This allows a timely entry to e-commerce.

The online store consists of the shopping solution in the front-end, and the payment processing, shipment and marketing management modules at the back-end. The first six months online explore are accompanied by five workshops. The first workshop is the kick-off workshop for setting up the project plan and the terms required by the future online company and HP would support the initiative of this feature. Once the resources are provided and the project plan are decided, the second workshop -- marketing will be used to develop the marketing strategies. Right after this second one, a workshop is on the agenda that will explain the e-commerce solution to the company. After the first three workshops are completed, the digital shop is ready to go online to the public. Then an intermediate workshop the fourth one is planned after three months' exploration, and all the interim results are analyzed and discussed with the company staffs. The final

workshop analyses the performance of the six months' experience and discusses the future further steps. Thereafter the company opens a planned digital online store and it can make a decision that let HP host its solution, handle the solution over an ISP or handle the solution in its own environment.

3. BroadVision One-to-One Commerce

BroadVision One-to-One Commerce [12][20] is an extensible and flexible electronic commerce application that helps companies to make selling more efficiently to their companies' online shoppers, no matter they are consumers, businesses, or channel partners (B2B, B2C, Peers). With its instant personalization features, it enables fast-moving, high transaction companies to instantly change their products, prices, promotions, announces and other contents to better meet their user's needs.

The application's comprehensive shopping engine allows the companies to create the best shopping experience for their customers no matter how depth the computer basic knowledge they have. The system enables the full integration of enterprise, payment, and shipping systems to merger with their existing investments and service. The site management tool is easy to use and allows business manager to change incentive, adverts, products and other contents without having to know much about the underlying technology. The catalogue and content management tools enable business managers to

add, change, stage and publish content from wherever they are through a simple-to-use friendly user interface (UI).

4. Microsoft Commerce Server

Microsoft Site Server 3.0 Commerce Edition [12][21] is the solution of Microsoft to the e-commerce problem. This application is highly integrated into Microsoft BackOffice and its development tools. Simple sites can be designed by only modifying some basic templates, while complex sites can be designed and customized through the use of Microsoft Visual InterDev.

Bundled with Microsoft SQA Server, which gives the company a complete database package. Building into the software is so-called as pipelines, which are visual models that allow the company to manipulate the order of the business processes. Two types of pipelines are available: One for the e-commerce online shopping solution and the other is for the ORM (Object Role Modeling) type of business-to-business solution. As all servers' features can be scripted and programmed through COM (Component Object Model) objects, the pipelines can be extended to adapt to any scenarios. However, this requires an in-depth knowledge in the Windows platform and the product itself. Using the GUI (Graphic User Interface) pipeline editor, users have the ability to tweak or add code to various steps along the way, once the whole business pipeline has been implemented.

Cross-promotions are supported natively by the system. Any combination of rules and database fields can be used to create special sales, cross promotions and customer-based promotions. It also offers a web site analysis tool that gives the user (a company) feedback on how many customers are using the site and what their preferred products are so the company can change or make its business strategies.

5. Open Market LiveCommerce

LiveCommerce by Open Market [22] is an Internet application that uses an embedded object-oriented database technology to generate a very flexible enterprise-scale catalogue system. LiveCommerce is designed for very large catalogues with up to 100,000 items. It offers a fast and flexible navigation capability and offers customized searches according to the customer's requirements by generating the desired catalogue page for the browser.

It is possible to use LiveCommerce as a stand alone Internet catalogue system. But it will have a better solution when it integrates with other existing systems, such as the transaction and inventory system. The latest release version incorporates a new store setup wizard, making it even easier for small to medium sized merchants to take advantage of the features. Dual currency support has been integrated to present prices of the features at the same time, such as Deutsche Mark and Euro.

6. Yahoo Store

The Yahoo Store [12][23] is a special application of e-commerce that could not be bought, only available for renting. This special application resides on the Yahoo-Server and merchants are able to administer their shop via the normal web browser. It uses an intuitive interface. It has a built-in search engine and offers peerless statistical tools. The pricing options are very powerful and flexible. The rental price depends on the number of items, which a merchant wants to sell via the online shop charged as a monthly fee.

Depending on their (the merchant) focus, it may make sense to outsource the hosting of the web server and the shopping software. In general, a company will outsource all parts that are not strategic for it. If shopping is just an add-on to the core business, then this could be a good solution to choose.

7. Intershop Online

The Intershop [24] solution offers a complete, open shopping software package. It consists of ready-to-use templates that can be used to create the layouts for the shop so the company doesn't have to spend a lot of time to focus on its early plans. The standard search and index functionality are also available. In addition to this, customers are able to register their address and payment method. These data are saved for returning customers. Promotions and pricing can be configured easily at any time through the friendly web

administration interface. Payment methods, which are already pre-integrated, include SET and SSL credit card payment, invoice and cash on delivery, and those also can be easily extended.

8. EIMedia NetSell

NetSell [25], developed by ELMedia, is an application that is simple to use. The administration is done through a normal web browser, and updates are made directly to the production data. These capabilities make this application suitable for smaller shops with only a few products. Larger shops won't want live updates; and they will need a staging area, where they can test the changes first. A shopping basket and a customer database for registered customers is available. The NetSell solution is designed to work at an ISP site, which hosts the web server and the shopping software.

Basic features of an e-commerce application

Not every e-commerce application includes all the required features. In most cases, some additional programming is required to implement special processes. The basic components, needed by an e-commerce application could be found in Table 5-1. A customer entering an online shop should immediately grasp what type of shop it is. In order to make shopping easy, a shopping basket is required. Otherwise, the customer requires check out every single item they brought.

perhaps a 100 percent markup to the wholesale, another 100 percent to the retailer. A 50-percent-off sale at Saks may still have left a dress or a suit at twice the price it cost leaving the factory, which in turn may have been twice the price of labor and the fabric that went into it. In another words, if a dress original price from factory is \$ 100, and the wholesale price is about \$ 200, and the retailer will mark \$ 300 for it. So even the huge discount was given by retailer around 50 %, the consumer still need to pay \$ 150, which is much high than its direct cost from factory. This is a simple comparison but the result is obviously clear to see by the consumers.

In the 1990s there were 18.6 square feet of retail space for everyone in the United States that is twice the amount of two decades earlier. And whereas every square foot generated an average of \$175 in sales in 1975, 20 years later it only generated \$166, and this is \$ 9 in difference. At the same time, expenses were skyrocketing. Even the superstores were not looking so super in comparison with cyber retailers (such as Amazon.com, it was reported first ever profitable on April, 2002 [15]), who populated a market no less competitive yet far more immediate and omnipresent than any physical shopping district. A cyber retailer could easily reduce its expenses to barely 14 percent of its revenues, while normal operating costs relative to sales were rising at almost every traditional retailer no matter where it is. At the same time that operating costs and sale prices were plunging in the interactive marketplace. A cyber retailer could be leaping over traditional providers of goods and services to build a global presence for hundreds of millions of traditional buyers. With no inventory, no display space, and no old-fashioned stores to

service, sales per square foot had become irrelevant for the cyber retailers of 2008. And the new generation of shoppers in cyberspace found no full parking lots, no jostling crowds, and no “sold out of size 14” sign.

At the old-fashioned store in the late twentieth century, there were perhaps 30 models of portable stereos on display with ten brands and each with three or four speaker configurations. Buying such system in 2008, you are the consumer can simply suggest to your personal agent (possible are the few click buttons from online shop) that you want the speakers to be separable. In a flash, all those models with stationary speakers disappear from the “shelves” and the full list of the products with your demands display on screen just in front of your eye at home. And additionalLet’s say that your additional demands are you want a twelve-disk CD changer and built-in optical fiber connectors. Just in a few seconds, there are in front of you with over thousand models available and the best five displayed with brands, product information and prices. The entire process (cyber shopping) has taken less than 10 minutes of your time. Before you could even have gotten the attention of a hurried clerk with five other customers waiting to elbow you out of the way, you have found the portable stereo system that suits you best. Your family and yourself will be listening to it at next day evening’s family big event. Not only will your purchase be delivered promptly to your doorsteps, and it will be there at a price 20 percent below the best price on the shelf of a national discount store and also it will be without sales tax at the most purchase. Why? No rent and no salesperson to pay, no heating bills or parking lot attendants, and no inventory to float. Instead of a salesperson,

the cyber retailer becomes an information and mediating agent. This is new shape of the new “mall” of cyberspace. Who is populating it, and what are they buying? What do they expect? What will it take to sell to these buyers?

With this super shopping mall combines with other available components (At 2008, most of the families at United States have the Internet connectivity with broad bandwidth and such product—WebTV and Compaq’s cable-ready personal computer.), time spent over shopping activity becomes less whereas more money spent on this shopping activity. From the “cyber marketplace” shoppers can get almost everything for their daily life needs, home office suppliers, or business suppliers only by few mouse clicks.

Although from January 2000 through June 2001[16], the big wave hits on this industry and total of 555 e-business-related company shutdown their sites and venture capitalists declines their invest in Internet companies. It looks like a dark period ever. Let’s look at the technology industry back in the late 1980s, after the market crashed on Oct. 19, 1987. It was a very, very dark five years for the technology industry, but it was also one of the most important times for technology companies to restructure themselves. As a result of restructuring companies, they are successful after that. During the first half of 2001, California has 107 Internet companies and during the same period of time, New York has only 52 companies that close their business doors. There may be good news for B2B and B2C Internet sites alike that there were only 32 shutdowns in July 2001, declining from 58 in the pervious month.

There was too many negatives in 2001 about the Net that everyone missed an important trend -- e-commerce rocked on. Despite the massive fallout of dot-coms, people increasingly bought more things on the Net. According to Forrester's Online Retail Index [14], consumer sales hit US\$47.6 billion in 2001, a 12 percent increase over the previous year. On the business-to-business side Forrester found that the average amount of materials bought online by companies jumped from 7.1 percent of all purchases in the third quarter of 2001 to 9.5 percent in the fourth quarter. The Net has become a bona fide channel, not a novelty. So, with all of the thrill and excitement gone, companies need to get back to business and figure out how to make the Net working for them. Those are all good signs. That means, e-business is getting out from the dark side and still has very bright future.

GLOSSARY

Asymmetric key cryptography When one key is used to encrypt a message and a second key is used to decrypt the message, the key-pair indicates the use of asymmetric key cryptography.

Authentication. The process of authenticating that a message received came from the entity whom the recipient believes to be the sender.

Authorization A process whereby transactions are approved or declined by the card issuers. Successful authorizations reduce the amount of available credit but do not actually charge the customer, nor move money to the seller. Authorizations can be performed via telephone, POS terminal, or the Internet.

Cryptosystem A system disguises messages such that only selected people can see through the disguise.

Cryptography It is the science (or art) of designing, building, and using cryptosystems. It comes from the two Greek words *krupto* and *graph* that means secret and writing.

Cryptanalysis It is the science (or art) of breaking a cryptosystem.

Cryptology It is the umbrella study of cryptography and cryptanalysis.

Cryptographic Key A series of data bits that are used to control a cryptographic process, such as encryption, decryption, or message authentication testing.

Digital Certificate The binding of an entity's identity with a public key, performed by a trusted party. Required for PPK cryptography purposes.

Digital Signature Created using PPK cryptography and message digests.

Encryption allows a message sender the ability to digitally sign messages, thus creating a digital signature for the message. When a message digest is computed and then encrypted using the sender's private key, and later appended to the message, the result is called the digital signature of the message.

Electronic Commerce (e-commerce) Electronic forms of communication that permits the exchange of sale information related to goods and services purchasing between buyers and sellers.

Encryption The hiding or masking of information through cryptography such that only those permitted can see through the disguise.

Message Digest A unique fingerprint of a message that's calculated based on the contents of the message using a hashing algorithm. The original message cannot be recovered from the message digest, but is used to verify that no changes to the message took place while en route to the recipient.

Key-Exchange Certificate One type of digital certificate that's used to share the public key with those intending to send messages to the certificate owner. Contrasted with Signature Certificate.

Private Key The half of a key-pair that's retained on the computer which generated the key-pair. Private keys are used to encrypt messages that can be verified as legitimate if the associated public key is able to decrypt them.

Public Key The half of a key-pair that's shared with message recipients to use in sending encrypted messages back to the private key holder.

Public/Private Key-pairs A required component for Public-Private Key (PPK) cryptography whereby two mathematically related keys are used to encrypt and decrypt communications between two or more parties.

Signature Certificate A type of digital certificate that is used by the message recipient in authenticating the origin of a signed message. Contrasted with Key-Exchange Certificate.

REFERENCES

1. David Bollier. 1998. *The Global Advance of Electronic Commerce reinventing markets, management, and national sovereignty*. The Aspen Institute.
2. Walid Mougayar. 1998. *Opening Digital Markets: battle plans and business strategies for Internet commerce*. McGraw-Hill.
3. Samantha Shurety. 1999. *E-Business with Net.Commerce*. Prentice-Hall, Inc.
4. Jill H. Ellsworth, Matthew V. Ellsworth. 1994. *The Internet Business Book*. John Wiley & Sons, Inc.
5. Daniel Minoli, Emma Minoli. 1998. *Web Commerce Technology Handbook*. McGraw-Hill
6. Mark S. Merkow, Jim Breithaupt, Ken L. Wheeler. 1998. *Building SET Applications for Secure Transactions*. John Wiley & Sons, Inc.
7. Soon-Yong Choi, Dale O. Stahl. 1997. *The Economics of Electronic Commerce*. Macmilla Technical Publishing, Indianapolis, Indiana.
8. Browning Rockwell. 1998. *Using The Web to Compete in A Global Marketplace*. John Wiley & Sons, Inc.
9. Derek Leebaert. 1998. *The Future of The Electronic Marketplace*. The MIT Press.
10. Net.Gennesis Corporation. 1996. *Build A World Wide Web Commerce Center—Plan, Program, and Mange Internet Commerce for Your Company*. John Wiley & Sons, Inc.
11. Paul May. 2000. *The Business of Ecommerce: from Corporate Strategy to Technology*. Cambridge University Press.

12. Daniel Amor. 2000. The e-business revolution: living and working in an interconnected world. Prentice-Hall, Inc.
13. The Wall Street Journal
14. San Jose Mercury
15. San Francisco Chronic
16. <http://www.bcentral.com/resource/articles/line56/default.asp>
17. <http://www.oracle.com/oramag/webcolumns/2000/index.html?howwapworks.html>
18. <http://www.ibm.com>
19. <http://www.hpemporium.com>
20. <http://broadvision.com>
21. <http://www.microsoft.com>
22. <http://www.openmarket.com>
23. <http://store.yahoo.com>
24. <http://www.intershop.de>
25. <http://www.elmedia.de>