CHAPTER 2
RESEARCH METHODOLOGY

2.1 Introduction

This study employs both analytical and descriptive type of methodology. This study is done to fulfill the gaps identified in the literature survey. It is done in two stages with a preliminary pilot study followed by the main study. The various procedures followed in the research methodology are presented below.

This research has been divided into two broad areas namely Analysis phase and Improvement Measures phase. In Analysis phase, 25 sample sites are identified. An on-line survey is conducted among them. This is used to find the major areas in majority of the sites that requires improvement and to analyze the list of products commonly purchased and sold in commercial web sites and the level of security involved in them. In the second phase, the improvement measures are identified in the e-business. For this purpose, a framework is suggested and the factors are identified.

2.2 Site Selection

As mentioned above, to proceed with the study, the commercial sites have to be chosen for the analysis. The web sites are classified according to the volume of traffic, number of pages retrieved, frequency of transactions, complexity, and type, number of searches, information stability and security concerns. In any type of business, user satisfaction is a common measure of success. Hence, web sites should also be designed by keeping user satisfaction in mind. Figure 2.1 depicts the criteria for identifying user-based design.

The Contents of this chapter is published in International Journal of Computer Trends and Technology (ISSN: 2231-2803), Volume 1, Issue 2, May-June 2011, pp61-64. The reprint is appended toward end of this thesis.
Fig. 2.1. User based Design Criteria

This propose five types of high-volume web sites like publish/subscribe, online shopping, customer self-service, trading and B2B. In this research, publish/subscribe, customer self-service types are excluded. The Web site classification is shown in Fig 2.2.

![Diagram of User based Design Criteria]

Fig 2.2 Web Site Classification
To carry on the research activity, 25 commercial web sites are selected at random that are generally familiar among the users. A list of merchants and buyers are identified in these web sites. Then a questionnaire is prepared with a set of multiple choice questions. They are circulated among the users of the web sites through e-mail and the filled in survey questions are collected back on-line. This survey is meant to find the demand for the products, security involved, mode of advertisement, and to get suggestions from buyers and sellers. The survey results provided an opportunity to understand customer problems, market trend, customer preferences, list of products that have less demand, expectations from the customers, risks involved in e-commerce transactions, customer’s preference in payment mode etc. The following are the criteria used for site selection:

- Payment method practiced
- Security measures considered for effective transaction
- Delivery mode practiced
- Variety of items sold
- Types of services provided in the site
- User friendliness of the web sites
- Marketing trend followed in the sites
- Legal issues in the web site

The web sites that match these criteria are identified from internet, television and newspaper media. Among them 25 are considered at random for the purpose of survey.

The following are the 25 web sites that are taken as sample:

- www.ebay.com
- www.amazon.com
- www.alibaba.com
- www.fabmart.com
- www.shopping.rediff.com
- www.sifymall.com
- www.shopping.indiatimes.com
- www.indiaplaza.in
- www.homeshop18.com
- www.futurebazaar.com
- www.indiavarta.com
- www.makemytrip.com
- www.yatra.com
- www.music.today.in
- www.thehindushopping.com
- www.shoppingchennaionline.com
- www.bookmyshow.com
- www.chennaionlinegrocery.com
- www.onlinestore.net.in
- www.saravanastoresnew.com
- www.magicbricks.com
- www.inidaproperties.com
- www.shopping.yahoo.com
- www.fnp.in
2.3 Research Design

It has been decided to carry out the research activity in two different phases. The first phase is the analysis phase and the second phase is the improvement measures phase. The analysis phase is based on the answers obtained from the questionnaire in the survey.

The sample size is taken as 750 buyers and 750 sellers at random from all the participants in the survey. The completed questionnaire containing answers for all the questions alone is identified and considered as sample. The analysis tool SPSS is used for analysis. Factor analysis, cluster analysis, ANOVA, Data analysis, non-parametric chi-square analysis are used for analyzing the user data.

The second phase is to identify the improvement measures in e-business by improving the web design architecture. For this purpose, a new architecture is proposed. That is, there could be just one master web site taking care of all the transaction among all the websites in the world. Users who wish to purchase items from different web sites need not get inside each and every web site. For instance, a person may wish to buy books from www.amazon.com and a gift item from www.ebay.com. The normal process is that he should get inside www.amazon.com and submit his credit card details for payment and get the item. Similar process is repeated by the user in www.ebay.com or any other web site. It is a time consuming process because the payment gateway process and checking for authentication, authorization and security must be repeated in every site where the purchase is made. Also every web site owner should pay for the payment gateway.

But the proposed framework will overcome all these difficulties. There could be just one general master web site providing link to all the other web sites in the world. The merchant who wish to sell his items must become a member of this web site. The membership is given by the master web site after complete authentication.
and authorization process using highly secured cryptographic algorithms like RSA. This creates a digital certificate for the merchant with digital signature. The digital certificate contains the name of the merchant, unique identification number, period of membership etc. The membership period can range from a minimum of 1 year to 3 years. Accordingly, membership amount is charged by the master web site owner.

The benefits of membership are as follows:

- Any type of legally authorized products can be sold from this web site
- The merchants need not pay separately for the payment gateway since the payment gateway process is done by the master web site itself
- The advertisement cost is minimal since he does not maintain a separate marketing channel.
- The merchant need not bother about receiving money for the items sold because this is taken care by the master web site.
- Verifying the authentication details of the users need not be done because it is taken care by the master web site.
- It empowers more security to the merchant.

The same process is repeated for the users/buyers in the web site. The buyers first enter into the master web site. It is like a multi shopping complex where they can buy any item from any merchant and from any place. Once the items are selected from the various web sites, the payment details are accepted from the user. The credit card details and other personal information are collected by the master web site and sent to the payment gateway. It need not be submitted in each and every web site. Hence, confidential information is given at only one place. Thus this framework improves the accessibility of the web sites available and in turn it also improves the e-business.
2.4 Questionnaire Design

To carry out the research activity, two sets of questionnaire are designed separately for buyers and sellers. The questionnaire consists of multiple choice questions and yes or no patterns. They contain the questions related to the issues given below.

- Types of products sold or purchased in the e-commerce web sites
- Number of years associated with e-business
- Payment method followed
- Mode of delivery or mode of purchase of goods
- Attractive features identified in the web site
- Speed of transaction
- Security measures followed in the transaction
- Difficulties felt in buying or selling of products
- Selection mode followed in the web sites
- Business done in auction mode
- Suggestions from the users

Each set of the questionnaire consists of 50 questions. From the web sites, the e-mail id of the customers is identified. The questionnaire is mailed to them through internet. The respondents are requested to give their opinion and complete the questionnaire. The completed questionnaire is received back again through e-mail. The survey provided an overall solution to the following:

- Quantitative and qualitative indicators used to measure the overall results of implementing e-commerce solutions.
2.5 System Design

The following section depicts the system design followed in this research work. The seller first registers himself with the SETS Framework and obtains the digital certificate for a specified period ranging from 1 year to 3 years. After the registration, the link is provided in the master web site. The users can browse into any of these registered sites and purchase any type of product. This is represented in the Fig. 2.3.

After selection, the items are added into the shopping cart. The payment details and mode of payment and confidential information related to payment are submitted to the SETS model. The details are forwarded to the payment gateway for further processing. The processed information along with the amount is sent to the SETS model. The SETS framework makes payment to the seller for the items sold and purchased by the buyer. Thus, in this model all communications are only with the SETS framework and not between the parties.

Fig 2.3 Scenario of the web site

After selection, the items are added into the shopping cart. The payment details and mode of payment and confidential information related to payment are submitted to the SETS model. The details are forwarded to the payment gateway for further processing. The processed information along with the amount is sent to the SETS model. The SETS framework makes payment to the seller for the items sold and purchased by the buyer. Thus, in this model all communications are only with the SETS framework and not between the parties.
There is no communication path between the buyer and seller and between seller and payment gateway or between buyer and payment gateway. The SETS framework takes care of all types of communications from every one. This is represented in the fig 2.4.

![SETS Process Diagram](image)

**Figure 2.4 SETS Process Diagram**

The authentication of the buyer and seller information is more important to provide security to the e-commerce transactions. The authentication can be classified into 2 types as:

- Seller Authentication
- Buyer Authentication

Seller authentication is required to determine if the seller has the privilege to participate in an e-commerce transaction. The authentication is done for a specified
period of time as requested by the seller. Accordingly subscription amount is charged for the services to be provided in the requested period. The subscription amount includes the following:

- Processing of user transactions
- Making Payment to the merchants for the purchases made by the users
- Authenticating the merchants for the services they provide
- Providing a unique Identification for the merchant in the multi shopping environment

Authentication is done on the following pairs:

1. Seller, SETS server
2. Seller, Merchant content provider MCP
3. MCP, Policy server (PS)
4. PS, SETS server

Merchant content provider (MCP) is a server that provides the details of a seller to the users. The seller maintains about the details of products to be sold. It includes the product name, price and the stock level of each product.

The policy server (PS) maintains the general policies to be followed by each seller based on the location, currency etc. It also contains the service policies of each seller in a transaction. Thus, the authentication is done between the seller and SETS model, payment gateway, policy server and merchant content provider. After authentication, the sellers find an entry in the master web site. The buyer can buy any item from any of the web site. The payment details are collected and encrypted and the hash value of them is found. The hashed data is sent to the payment gateway for processing.
To ensure confidentiality in processing, a nonce value is generated from both the framework and the payment gateway. The nonce value is a randomly generated value which will be the same value on both sides. The nonce value will be kept secret. The value is matched along with other parameters for equality. Thus, secrecy is maintained at a higher level. When they are matched, the payment gateway will signal with yes/no response to the framework. Accordingly, the transactions are processed. The transaction details with each merchant are noted in a temporary database. When payment is made to the framework through the payment gateway, the amount is settled for all the merchants by the framework.

Advantages of the framework:

• The subscribers can do shopping from any of the available websites in the framework.

• Network traffic is highly reduced between the framework and the payment gateway.

• The seller need not pay anything for the payment gateway.

• Authentication and Authorization is done only once in the framework.

• The subscription amount to the SETS framework paid by the Seller is comparatively less than the amount paid to the payment gateway if it has to be paid by each seller.

• It provides a development platform for the fast and cheap development of secure and reliable e-commerce services in the Internet.

• The framework settles the amount for the purchases made by the buyer.

Limitations of the SETS framework:
As new web sites are coming day by day at a faster rate, the domain space for accommodating in a single server is not possible. Cascading servers and other emerging new technologies can be used to partition the space and distribute them in various servers.

Every seller may not wish to subscribe for the framework by making payment for subscription.

The seller may require unique identification by having a own web site. The seller may not like to come under the supervision of a master web site.

In spite of these limitations, the framework helps to speed up the process of purchase in the consumer's point of view. Also marketing and advertising cost and payment gateway process is also reduced. This ensures the improvement of e-business.

2.6 System Modules

The SETS framework is developed as a mini software project for implementation. The following are the various system modules.

- Authentication Process
- Product purchase process
- Payment gateway process

2.6.1 Authentication Process

The authentication process is the first module in the framework. It is used to authenticate the seller in the e-business. For the purpose of authorization the following details are accepted from the seller:
• Type of products sold and their legal issues
• Period of membership required
• Nature of business
• Mode of delivery to be followed
• Brand of the products sold and their quality etc

These details are encrypted using highly secured algorithms and stored in Merchant Content Provider. The details are also used to create a digital certificate containing the digital signature of the issuing certification authority. This possession of the digital certificate is mandatory for every seller and this provides authentication for him to do business.

The buyers from this web site are also provided with an option to view the digital certificate. By clicking the option, the buyers can view the digital certificate of the sellers and trust their sales. It is a stronger authentication mechanism as compared to a password-based authentication mechanism, because the user is expected to have a certificate. The following are the summary of steps involved in Certificate-based authentication system:

Step 1: The merchant is requested to fill a Registration form. This form contains the details about the subscription date, period of subscription, web site address etc. They are stored in a database after confirmation.
Step 2: Creation, storage and distribution of digital certificates. It is shown in fig 2.5.

The digital certificates are created by the Certification Authority for each user and the certificates are sent to the respective users. A copy of the certificate is stored by the server in its database. This is needed to verify the certificate during the user’s certificate based authentication. This certificate contains the Merchant id, Certification Authority’s digital signature, subscription date, validity period etc.

Step 3: Server creates a Random challenge

After receiving the purchase initiation from the buyer, the server checks to see if the merchant is valid. If it is valid, the server now creates a random challenge and sends it back to the user.

The random challenge is the secret text/information that is created at random for security purpose. It travels as a plain text from the server to the user’s computer.
Step 4: Signing the random challenge. The SETS encrypts the random challenge with the user’s private key to produce the digital signature of the merchant.

Thus authentication helps to provide a trusted network in e-business.

2.6.2 Product Purchase Process

2.6.3 Before the transaction begins, the cardholder is assumed to have completed browsing, selecting and ordering of the items from the various merchant’s site. This transaction is made up of four messages. They are: ...
1. Initiate Request
2. Initiate Response
3. Purchase Request
4. Purchase Response

Step 1: Initiate Request:

![Diagram]

**Figure 2.8 Initiate Request**

The Initiate request process is done by the buyer to the seller. To proceed with the transaction, the buyer would like to view the digital certificate of the seller. This contains the authentication details of the seller and thus enables the buyer to proceed with a safe transaction.

Step 2: Initiate Response:

![Diagram]

**Figure 2.9 Initiate Response**

The initiate response process is performed after the initiate request process. As per the request made by the buyer, the seller displays his digital certificate and his unique transaction id. This strengthens the confidence level of the buyer to make purchases with the seller.
Step 3: Purchase Request:

This purchase request is done again by the buyer after selecting the items for purchase and adding them in the shopping cart. This purchase request contains the following:

- Order Information (OI) containing the order id
- Digital signature calculated over OI
- Message digest over OI called OIMD

All the above information is encrypted with the private key $k$ of the seller.

The seller is verified as shown in fig 2.10.

![Diagram of step 3: Purchase Request](image)

**Figure 2.10 Verification of Seller’s Authenticity**

The seller calculates his own OIMD (Message Digest of Order ID) and the PIMD (Message Digest of Purchase Initiation) received from the buyer to generate his own POMD (Message Digest of Purchase Order). The POMD is also calculated by the buyer in the same way in the encrypted form and is called POMD2. The framework decrypts the Digital signature DS received from the buyer to retrieve the POM2D as was calculated by the user. The seller compares the POMD1 and POMD2 and if they are equal it trusts the message.
Step 4: Purchase Response:

When the purchase request is received with the encrypted information, the framework does the following:

- Verifies the buyer’s certificate by means of (CA) Certification Authority signatures
- Verify the signature created over PI (Purchase Initiation) and OI using the user’s public key
- Process the order and forward it for payment
- Send a purchase response back to the user. The response may be positive or negative as per the processing details of the encrypted information.

Thus the above steps complete the product purchase process in the web site. For a higher level of authentication, protocol like RADIUS can be used. RADIUS stands for Remote Authentication Dial-in User Service.

RADIUS is a widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. The RADIUS packet with its codes is shows in fig 2.12.
Fig 2.12 Summary of RADIUS Packet

The code establishes the type of RADIUS packet. The various codes are shown in Table 2.1.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access-Request</td>
</tr>
<tr>
<td>2</td>
<td>Access-Accept</td>
</tr>
<tr>
<td>3</td>
<td>Access-Reject</td>
</tr>
<tr>
<td>4</td>
<td>Accounting-Request</td>
</tr>
<tr>
<td>5</td>
<td>Accounting-Response</td>
</tr>
<tr>
<td>11</td>
<td>Access-Challenge</td>
</tr>
<tr>
<td>12</td>
<td>Status-Server (experimental)</td>
</tr>
<tr>
<td>13</td>
<td>Status-Client (experimental)</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Thus by means of these, authentication can be made highly effective in this purchase environment.

2.6.3 Payment Gateway Process

This is the process where the amount for purchase is collected from the buyer. The buyer need not pay the amount directly to the seller. Rather, it is paid to a separate channel called the payment gateway. Generally, Payment gateway is an e-commerce service that authorizes the payment for all the transactions. It encrypts the sensitive information like credit card information.

It verifies the following details:

- Type of the Bank
- Credit limit
- Expiry date
- Type of card

Once items selected and before placing them in the shopping cart, the buyer is validated for the purchases to be made. Hence, the Certification Authority issues the digital certificate containing the user id for the buyer. After selecting the items and putting them in shopping cart, the mode of payment is selected. If it is cash payment then payment gateway process is not required. The cash can be paid directly to the person at the time of delivery of the products. In case of credit card or debit card payment, the payment gateway is required to authorize the payments. It collects the amount from the buyer and sends the amount to the framework.

The buyer can buy different items from different sellers as the same time. For example, the buyer can buy items for Rs.1000 from seller A, Rs.2000 from seller B and Rs.3000 from seller C. The buyer makes the total payment for all the purchases i.e. Rs.6000 to the framework. The framework maintains the details of payments to be
made to the seller A, B, C by the buyer. Accordingly, the amount Rs.1000, Rs.2000, Rs.3000 is send to A, B, C respectively.

The payment from the buyer is validated by generating nonce values for the payment gateway and the SETS. The hash value of the nonce, private key of the SETS and the private key of the payment gateway are encrypted. The Object identification, amount to be paid are verified are compared in the database of the framework and sent to the payment gateway. After validation and verification of the transaction amount details, the payment gateway returns an appropriate message to the SETS saying whether the buyer is eligible to purchase or not. The eligibility criterion is based on the credit limit, validity, amount of purchase etc.

Without this framework, every web site should pay for the payment gateway for processing the credit card or debit card details. Hence, network traffic is more and cost is also more. But, in this set up, it the sole responsibility of the SETS to pay for the payment gateway. Every web sit owners need not pay for the gateway but only they have to pay for the subscription period to the framework. The SETS alone pay to the payment gateway.

Hence, it is cost effective and a highly secured set up.

2.7 System Architecture

The system architecture of this framework represents the various components used in this model. They are certification authority group, certification authority, payment gateway, buyer and the seller.

The certification authority group consists of the members for processing the certification request. The request may be for getting a new certificate or renewing the existing one. The payment gateway is used to process the payment details. The buyer and the seller are the main members in the commercial transactions.
All the components are inter-connected. The request and response are generated for authorization and issue of certificates. The architecture is represented in fig 2.13.

2.8 Data Flow Diagram

The Data flow diagram represents the general flow of data from one module to other. It shows the type of data generated in every process. The circles represent the process name and the arrows carry the name of data that flows from one process to other. The rectangles represent the database which is the storage place of various data in a common form. The request is sent from the buyer and from the seller to the model.
The buyer and the seller request the SETS model to proceed with their process. The SETS model generates the public and private keys and they are sent to the authentication process. The authentication is done in authentication process and the details are sent to the buyer and seller. The authentication process also issues the digital certificate to the seller. The items selected by the buyer are added to the shopping cart and the details are sent to the purchase process.

The purchase process validates the purchases done by the buyer and the credit card and debit card details are sent to the payment gateway process. The payment gateway validates the transaction details and ensures the payment details. The valid transactions are to the payment process. The fig 2.14 represents the data flow diagram for the SETS model.

Figure 2.14 Data Flow Diagram

Thus this chapter summarizes the area of study, system design, and systems architecture and data flow diagram. The sample output of the system is given in Appendix 3. The next chapter presents the analysis of the data collected from the buyers and their findings.