TWO FACTOR AUTHENTICATION USING MOBILE-PHONES

for
Department of Computer Applications, CUSAT

A
Project Report
Submitted for partial fulfillment of the degree of
Master of Computer Applications

By
Kavita Kumari Jethwani

DEPARTMENT OF COMPUTER APPLICATIONS
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY
Kochi- 682022
Kerala.
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY COCHIN-22

Project Work

(Sixth Semester)

TWO-FACTOR AUTHENTICATION USING MOBILE PHONES

Bona fide record of work done by

KAVITA KUMARI JEHWANI
Reg. No. 95580018

Submitted in the partial fulfillment of the

Requirements for the award of the degree of

Master of Computer Applications

Of Cochin University of Science And Technology

APRIL 2011

__________________________  _____________________________
Faculty Guide                                                     Head of the Department

__________________________  _____________________________
Internal Examiner                                                  External examiner

Submitted on: __________________
ACKNOWLEDGEMENT
ACKNOWLEDGEMENT

This Project itself is an acknowledgement to the inspiration, drive and technical assistance contributed by many individuals. This project would have never seen the light of this day without the help and guidance I have received.

First and for most I wish to express my sincere thanks to Almighty God for his blessings showered on me throughout this endeavor.

I would like to express my profound thanks to Dr.K.V.Pramod, the Head of the Department of Computer Applications, Cochin University of Science And Technology, for his help and guidance throughout my project tenure.

I am grateful to Pentech Solutions Pvt. Ltd. For giving me an opportunity to carry out a full semester project.

I express my sincere and heartfelt thanks to Mr. Gokul Kumar J, Branch Manager, Pentech Solutions, for giving the opportunity to do this project.

I am grateful to Mr. Pradeep S, project guide for his valuable suggestions Guidance, support and co-operation throughout the project that help me to develop the system successfully.

I also express my deep gratitude to the faculty members Ms. Malathi, Mr.B Kannan, Mr. A. Sreekumar and other faculties for their valuable guidance, timely suggestions and help in the completion of this project.

I extend my heartfelt thanks to my parents, friends and well wishers for their support and timely help.
SYNOPSIS

The Two-factor Authentication using mobile phones system allows user or customer to use a personal password to confirm his identity and protect his/her card when the card is used on the Internet, providing greater reassurance and security. The proposed system is a security system that tells on-line retailers that the user is a genuine cardholder when he shops on-line.

To meet the user requirements, The proposed system incorporates the following features:

♦ In this proposed system specifically the example of online book shop is taken to represent the online transaction. After the selection of the book the user can select the credit card payment mode and enter the secured processing system(SPS) for secured transaction.

♦ During the online transaction process, the Merchant payment systems will connect to the sps system to carry out security, fraud and validity checks and subsequently authorize and take the payment. It improves the security of Internet payments by providing an additional password to the user. Using the password the user can successfully make his payment.

♦ Online card transactions over Internet need enhanced security. Secure processing system facilitates additional security by way of a cardholder-chosen password, which is known only to the cardholder.

♦ SPS is a new way to add safety when the user buy online. Adding a personal password to the existing Credit Card ensures that only the authorized card holder can use Card online. It's easy to activate the SPS service on your existing Card.
Whenever the user submits an order at a participating online store, the SPS window will appear. User enter details and the password will appear in the authorized mobile phone, enter the password in the appropriate box and submit, and payment is over.

SPS receives credit card details from the card issuing bank which is invisible to the customer. SPS provides verification details to the customer. It varifies the password and other details.

Cardholders enter their PIN on the key pad to generate a one-time code for secure authentication by SPS.

Dynamic passcode authentication is one solution that uses the added security of credit cards to offer better protection against online fraud. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses.

Thus the proposed system is adding an extra layer of security at the point where you enter credit card information online. The service helps to prevent unauthorized online use before it happens by confirming your identity with an additional password.

List Of Modules:

- User Interaction Design
- Server Validation and Process
- Database Interaction
- Generating OTP Algorithm
- GSM Modem Implementation
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

- **User Interaction Design**
  
  Developing the Graphical User Interface of View Layer in Java Server Pages for customers to login and select the items to purchase in web with Java Script Technology.

- **Server Validation and Process**
  
  Implementing the Model Layer of getting the inputs form the View Layer and processing of the Validation of Data logically in servlet Technology and forwarding the Response to Tomcat server in turn Display the corresponding view Page.

- **Database Interaction**
  
  Connecting the Database Driver used with Control Layer to validate the Request received from the Tomcat server and Responding the further process and is implemented Globalized such that the Database can be changed easily in code.

- **Generating OTP Algorithm**
  
  The card no and pin no from the view layer and Current Day, Date and time are take from the packages and implemented as parameter for the OTP Algorithm. As a Result it will generate the Dynamic Password

- **GSM Modem Implementation**
  
  GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. Importing the comm Driver and connecting the Modem to the PC with serial port.
CONTENTS

PREFACE

1 INTRODUCTION .............................................................................................................1

  1.1 ORGANISATION PROFILE ..................................................................................2

  1.2 PROBLEM OBJECTIVE ......................................................................................5

2 SOFTWARE QUALITY ASSURANCE PLAN ..............................................................6

  2.1 INTRODUCTION ....................................................................................................7

  2.2 OVERVIEW OF THE DOCUMENT ......................................................................7

  2.3 TASKS AND RESPONSIBILITIES ......................................................................8

  2.4 SQA IMPLEMENTATION IN DIFFERENT PHASES .........................................8

  2.5 DOCUMENTATION .............................................................................................9

  2.6 SOFTWARE DOCUMENTATION AUDIT .........................................................9

  2.7 REQUIREMENTS TRACEABILITY .......................................................................10

  2.8 SOFTWARE DEVELOPMENT PROCESS .........................................................10

  2.9 PROJECT REVIEWS .........................................................................................10

  2.10 TESTING AND QUALITY CHECKS ....................................................................10

3 SYSTEM ANALYSIS ....................................................................................................11

  3.1 IDENTIFICATION OF NEED ...............................................................................12

  3.2 PRELIMINARY INVESTIGATION(EXISTING SYSTEM) .......................................13

  3.3 PROPOSED SYSTEM ..........................................................................................13

  3.4 FEASIBILITY STUDY ..........................................................................................16

   3.4.1 TECHNICAL FEASIBILITY ..........................................................................16

   3.4.2 FINANCIAL FEASIBILITY ............................................................................17

   3.4.3 RESOURCE FEASIBILITY ............................................................................17

   3.4.4 OPERATIONAL FEASIBILITY ......................................................................17
INTRODUCTION
1. INTRODUCTION

1.1 ORGANISATION PROFILE

Pantech Solutions Pvt Ltd is one of south-India most well-known and well-trusted solution provider. Today, Pantech stands as a source of reliable and innovative products that enhance the quality of costumer's professional and personal lives.

Conceived in 2004, Pantech Solutions is rooted in Chennai and has its branches in Hyderabad, Bangalore, Cochin, Coimbatore & Madurai. Pantech is a leading solution provider in all technologies, and has extensive experience in research and development. Its 125 employees in all the metros of south-India are active in the areas of production, software development, implementation, system integration, and training.

Why pantech ?

With a client list spanning nearly in all industries, and colleges, Pantech Solutions’ product solutions have benefited customers of many different sizes, from non-profit organizations to companies. By acquaintance with Pantech you’ll have access to current IT research, tools, templates, and step-by-step action plans for completing Key projects. You’ll also be provided full access to our research archives and knowledge base.

Pantech Products :

1. Microcontroller Boards
2. DSP/DSC Boards
3. CPLD/FPGA Boards
4. Peripheral Boards
5. Power Electronics
6. Softwares

SERVICES :

- System Architectures
- Board design
- Software development
- Validation and testing services
SOLUTIONS:

Multimedia Solutions

Pantech Multimedia Solutions division specializes in website design and development, web-based information systems, flash and animations, e-commerce applications, Database creation, Web based applications, digital presentations and virtual tours.

Technology Solutions

Pantech Technology Solutions is a consulting division that advises and introduces, cutting edge technology based solutions to clients. This division aims to open the Southern African Business and the IT Sector as a whole to a variety of niche markets.

Technical Support

Pantech Technical Support Division not only Complements its other divisions by providing highly experienced technical engineers to support and maintain the various products and services but also outsource it’s expertise to other IT companies and Corporate. We offer our clients a wide range of services in new and traditional media. This allows you to select a holistic approach for your online marketing requirements. Whatever your solution requirements, we will develop it using a structured project management approach to ensure that the project arrives on time and within budget.

- Web Designing.
- Web Hosting.
- Web Maintenance.
- Web Re-Development.
- Personal Websites.
- search optimization.
- Hit counter.
- Client server technology.
- Image Capturing.
- Payroll.
- Customized Application Development.
- 3-tier & Multi tier Architectural Application Development.
- Multimedia.
- Corporate Film - With Concept, Production Design & Production.
- Logo Designs & Animation.
Customers:

Over the past 5 years Pantech products have improved the quality of communication and satisfied customers. We have earned their respect by providing excellent products and services. In addition, we are flexible with services and financial structures for contracts aiming for mutually beneficial relationships with our customers. Our customers are dynamic and diverse and include Large Corporate Offices, Universities, Educational Institutions, Factories, etc.

Our Customers:

<table>
<thead>
<tr>
<th>Customers Details</th>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. DRDO</td>
<td>NEW DELHI</td>
</tr>
<tr>
<td>2. NSIC</td>
<td>CHENNAI</td>
</tr>
<tr>
<td>3. ONE MEDIA CONTROLS</td>
<td>DUBAI</td>
</tr>
<tr>
<td>4. ALFA Sysems Pvt Ltd</td>
<td>BARODA</td>
</tr>
<tr>
<td>5. Colorjet India Ltd</td>
<td>NOIDA</td>
</tr>
<tr>
<td>6. Tessolve Solutions Pvt Ltd</td>
<td>CHENNAI</td>
</tr>
</tbody>
</table>
1.2 Objectives

The title of the project is Secure Processing System in Online Transaction. A Secure processing system is a security system that tells online retailers that the user is a genuine cardholder when s/he shops online. It allows user or a customer to use personal password to confirm his identity and protect his/her credit card when the card is used on the Internet, providing greater reassurance and security. It improves the security of Internet payments.

The objective of the proposed system is to make online transaction more efficient to the user who uses the website and shops online. This will have a positive impact on user profitability. To make on-line shopping even simpler and safer, a secure processing system is being introduced.

During the online transaction process, the Merchants payment systems will connect to the secure processing system to carry out security, fraud and validity checks and subsequently authorize and take the payment. It improves the security of Internet payments. To meet the business requirements, the proposed system incorporates the following features:

- Confidentiality of information
- Integrity of data
- Cardholder authentication
- Merchant authentication
SOFTWARE QUALITY ASSURANCE PLAN
SOFTWARE QUALITY ASSURANCE PLAN

2.1 INTRODUCTION

This document explains the Software Quality Assurance plan (SQAP) for Two Factor Authentication using mobile phones project. It is to provide the online shopping in secure manner.

2.1.1 Purpose

Software Quality Assurance Plan (SQAP) consists of those procedures, techniques and tools used to ensure that this product meets the requirements specified in Software Requirements Specification.

2.1.2 Scope

The scope of this document is to outline all procedures, techniques and tools to be used for Quality Assurance of this project.

This plan:

- Identifies the SQA responsibilities of the project developer and the SQA consultant.
- Lists the activities, processes and work products that the SQA consultant will review and audit.
- Identifies the SQA work products

2.1.3 Reference Documents

- Software Engineering, Roger S. Pressman, 5th Ed.

2.2 OVERVIEW OF THE DOCUMENT

The rest of the document is organized as follows:

Management: A description of each major element of the organization and a description of the SQA tasks and their relationships

Documentation: Identification the document related to development, verification, validation, use and maintenance of the software.

SQAP Requirements: This section defines the SQA reviews, reporting and auditing procedures used to ensure that software deliverables are developed in accordance with this plan and the project requirements.

1 Management

This section describes the management organizational structure, its roles and responsibilities and the software quality tasks to be performed.
2 Organization
Efforts for this project are supported by numerous entities, organizations and personnel. This tool is developed as part of partial fulfillment of requirements for Masters in Computer Applications degree. It will be the sole responsibility of the developer to review the product’s usability, efficiency, reliability and accuracy. The client will however conduct inspections, reviews and walk-through on a regular basis. Client specifications and suggestions will be used in places where quality decisions need to outweigh development schedule decisions.

2.3 TASKS AND RESPONSIBILITIES
- Develop the requirement specification and cost estimation for the project.
- Develop the design plan and test plan for testing
- Implement and test the application and deliver the application along with the necessary documentation
- Implement the test the application and deliver the application along with the necessary documentation
- Give a formal presentation to the client on completion of the analysis, design and testing phases. The client reviews the works and provides feedback/suggestions
- Planning, coordinating, testing and assessing all aspects of quality issues.

The responsibilities of the client are to:
- Review the work performed
- Provide the feedback and advice

2.4 SQA IMPLEMENTATION IN DIFFERENT PHASES
Quality assurance will be implemented through all the software life cycles of the tool’s development process, until release of the software product. The following are the quality assurance tasks for each phase of the software development:

Requirement Phase: When the SRS is being developed, it has to be ensured that it elucidates the proposed functionality of the product and to keep refining the SRS until the requirements are clearly stated and understood.

Specification and Design Phase: Due to the great importance for accuracy and completeness in these documents, weekly reviews shall be conducted between the developer and the client to identify any defects and rectify them.
Implementation Phase: The developer shall do code reviews when the construction phase of the Tool begins.

Software Testing Phase: The developer shall test each test case. The final product shall be verified with the functionality of the software as specified in the Software Requirement Specification (SRS) for the Tool.

2.5 DOCUMENTATION

In addition to this document, the essential documentation will include:

The Software Requirements Specification (SRS), which

- Prescribes each of the essential requirements (functions, performances, design constraints and attributes) of the software and external interfaces
- Objectively verifies achievement of each requirement by a prescribed method (e.g. Inspection, analysis, demonstration or test)
- Facilitates traceability of requirements specification to product delivery
- Gives estimates of the cost/effort for developing the product including a project plan

The Software Design Document (SDD)

- Depicts how the software will be structured
- Describes the components and sub-components of the software design, including various packages and frameworks, if any
- Gives an object model that is developed using Rational Rose highlighting the essential classes that would make up the product
- Gives a sample integration diagram, showing the key interactions in the application. This should also be a part of the object model.

Software Test Plan: Describes the test cases that will be employed to test the product.

2.6 SOFTWARE DOCUMENTATION AUDIT

Quality assurance for this project will include at least one review of all current work products in each stage of development (Requirement, Design and Implementation). The reviews will assure that the established project processes and procedures are being followed effectively and exposures and risks to the current project are identified and addressed. The reviews process includes:

- A formal presentation at the end of each development phase (Requirement, Design and Implementation). All current work products are presented to the client for review.
• A managerial review by the client periodically to ensure the work generated is in compliance with project requirements.
• Reviews by the client after each presentation

2.7 REQUIREMENTS TRACEABILITY

The SRS will be used to check off the deliverables. The Project Review will ensure that each of the requirements mentioned in the SRS is met by the deliverables.

2.8 SOFTWARE DEVELOPMENT PROCESS

The software development process involves three stages: 1) Requirement phase, 2) Design phase, 3) Implementation and testing phase. During each phase, the client will review the deliverables documents.

2.9 PROJECT REVIEWS

The client will perform a review at the 3 stages of the project as described in the section above. This review will determine whether the requirements have been met for the deliverable, check that the product meets requirements, ensure that the SQA plan has been adhered to, verify the performance of the software and ensure that acceptance testing is carried out. A design checklist will be used and the developer will check to see whether the design meets the checklist criteria.

2.10 TESTING AND QUALITY CHECK

Testing will be carried out in accordance with the Software Testing Plan (STP). Test results will be documented and discussed in the final phase of the project.
System Analysis
3. SYSTEM ANALYSIS

3.1 Identification of need

With growing usage of the Internet, people are utilizing the convenience of online shopping and the ability to place an order for what they want at all hours of the day and night, at the office, home, airport or just about anywhere. Services to the Internet will increase the business potential in many ways. However, e-commerce requires a commitment to securing transaction details, including credit card information from customers.

The following points emphasize need of the proposed system:

♦ When the user shops online and paying through credit card, the existing system does not contain any additional password security.

♦ In the existing system anybody can pay through credit card by providing the card pin number. He/She does not provide any additional information for online card payment.

♦ As e-commerce has grown, so have security threats. When the card is not swapped, it requires more security.

♦ The SPS provides additional information not visible in the card and facilitates the card holder to register their own password. That makes the user more secure while doing online transaction.
3.2 Preliminary Investigation

Dynamic passcode authentication is one solution that uses the added security of credit cards to offer better protection against online fraud. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses. The substantial proportion of customer complaints could be eliminated with the use of Authenticated Payment. This will have a positive impact on user profitability. To make on-line shopping even simpler and safer, a secure processing system is being introduced.

SPS is a simple password-protected identity-checking service that takes the risk out of online retail customers. The proposed system SPS is a new concept for additional security for all online ‘card not present’ transaction. In this concept when the card is not swapped, it require more security. Hence the SPS provides additional information not visible in the card and facilitates the card holder to register their own password. That makes the user more secure while doing online transaction.

Existing System

When the user shops online and paying through credit card, the existing system does not contain any additional password security.

In the existing system anybody can pay through credit card by providing the card pin number. He/She does not provide any additional information for online card payment. There is no assurance that only the right owner of the card paying through his card.

3.3 Proposed System

The proposed system allows user or customer to use a personal password to confirm his identity and protect his/her card when the card is used on the Internet, providing greater reassurance and security. The proposed system is a security system that tells on-line retailers that the user is a genuine cardholder when he shops on-line.

To meet the user requirements, The proposed system incorporates the following features:

♦ In this proposed system specifically the example of online book shop is taken to represent the online transaction. After the selection of the book the user can select the credit card payment mode and enter the secured processing system(SPS) for secured transaction.
During the online transaction process, the Merchant payment systems will connect to the sps system to carry out security, fraud and validity checks and subsequently authorize and take the payment. It improves the security of Internet payments by providing an additional password to the user. Using the password the user can successfully make his payment.

Online card transactions over Internet need enhanced security. Secure processing system facilitates additional security by way of a cardholder-chosen password, which is known only to the cardholder.

SPS is a new way to add safety when the user buy online. Adding a personal password to the existing Credit Card ensures that only the authorized card holder can use Card online. It's easy to activate the SPS service on your existing Card.

Whenever the user submits an order at a participating online store, the SPS window will appear. User enter details and the password will appear in the authorized mobile phone, enter the password in the appropriate box and submit, and payment is over.

SPS receives credit card details from the card issuing bank which is invisible to the customer. SPS provides verification details to the customer. It varifies the password and other details.

Cardholders enter their PIN on the key pad to generate a one-time code for secure authentication by SPS.

Dynamic passcode authentication is one solution that uses the added security of credit cards to offer better protection against online fraud. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses.
Thus the proposed system is adding an extra layer of security at the point where you enter credit card information online. The service helps to prevent unauthorized online use before it happens by confirming your identity with an additional password.
3.4 Feasibility Study

Feasibility study is the test of a system proposal according to its workability, impact on the organization, ability to meet user needs, and effective use of resources. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible.

The development of a computer based system or a product is more likely plagued by resources and delivery dates. Feasibility study helps the analyst to decide whether or not to proceed, amend, postpone or cancel the project, particularly important when the project is large, complex and costly.

Once the analysis of the user requirement is complement, the system has to check for the compatibility and feasibility of the software package that is aimed at. An important outcome of the preliminary investigation is the determination that the system requested is feasible.

The primary areas of feasibility analysis are:

- Technical Feasibility
- Financial Feasibility
- Resource Feasibility
- Operational Feasibility
- Economical Feasibility

3.4.1 Technical Feasibility:

The technology used can be developed with the current equipments and has the technical capacity to hold the data required by the new system.

- This technology supports the modern trends of technology.
- Easily accessible, more secure technologies.

Technical feasibility on the existing system and to what extend it can support the proposed addition. We can add new modules easily without affecting the Core Program. Most of parts are running in the server using the concept of stored procedures.
3.4.2 Financial Feasibility:

This system could be done with the current equipments and existing software technology. The cost for creating the system too is moderate and worthy.

- The hardware and software resources are easily available and so the project is financially feasible. No special investment is needed to manage the tool.
- No specific training is required for users to use the tool.
- The software used in this project is freeware so the cost of developing the tool is minimal.

3.4.3 Resource feasibility:

Our proposed project also have resource feasibility when it can be built, whether it interferes with normal business operations, type and amount of resources required, dependencies, etc. Contingency and mitigation plans can also be stated.

3.4.4 Operational Feasibility:

This proposed system can easily implemented, as this is based on JSP coding (JAVA) & HTML. The database created is with MySql server which is more secure and easy to handle. The resources that are required to implement/install these are available. The personal of the organization already has enough exposure to computers. So the project is operationally feasible.
3.4.5 Economical Feasibility:

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system. An entrepreneur must accurately weigh the cost versus benefits before taking an action. This system is more economically feasible which assess the brain capacity with quick & online test. So it is economically a good project.
4. SYSTEM REQUIREMENTS SPECIFICATION

4.1 Purpose

Services to the Internet will increase the business potential in many ways. However, e-commerce requires a commitment to securing transaction details, including credit card information from customers. As e-commerce has grown, so have security threats. Identity theft, data security breaches and phishing continue to top the list of consumer complaints. All of these factors undermine trust in digital commerce, and that is why it’s important for any small business to take the necessary steps to reduce customer concerns about shopping and banking online.

4.2 Scope

Transaction processing within an ecommerce environment, is the process of an online shop or ecommerce website accepting and processing a customer’s credit or debit card payment online and in real-time, in return for goods or services.

- Creates consumer preference to buy at online store.
- Educates customers and raises their comfort level with secure processing system.
- Authentication messaging helps prepare the customers for the authentication process.
- A dynamic password enhances consumer confidence.
- Cardholder alerts and avoids disruption in the transaction process and ensures the sale completes.

4.3 Applicability

It is critical that the payment gateway user choose supports basic fraud detection and that all required authentication measures are in place. For the most part, credit card fraud is carried out by individuals that have only the credit card number and not the physical card itself. Here are two authentication measures that payment gateway providers should have available.

- The Address Verification System authenticates a credit card purchase based on the billing address.
- The Card Verification Value supplying code in a transaction is intended to verify that the customer has the card in their physical possession.
4.4 Benefits and goals:

Benefits for Cardholder

- Increased consumer confidence when purchasing on the Internet.
- No special application software is needed at the cardholder access device (unless cardholder uses chip card).
- Easy to use.
- Control over card use for online purchases.

Benefits for Merchants

Ease of integration into merchant legacy systems.

- Minimal impact on merchant’s interaction with consumer.
- Increased sales by enhancing consumer confidence in online purchasing.
- Reduced risk of fraudulent transactions.
- Decrease in disputed transactions.

The secure processing system takes the submitted billing information from user customer’s computer, through secure server, and on to his merchant account at a processing bank. The gateway transaction is seamless and invisible to the customer, but to those concerned about security, it is anything but invisible. Thus it reduce the risk of fraudulent transactions.

Thus the benefits and goal of the proposed system is:

- Reduced risk of fraudulent transactions.
- Decrease in disputed transactions.
- Increased consumer confidence when purchasing on the Internet.
- No special application software is needed at the cardholder access device.
- Easy to use.
- Control over card use for online purchases.
REQUIREMENT

SPECIFICATIONS
5. REQUIREMENT SPECIFICATIONS

5.1 SOFTWARE REQUIREMENTS

✓ Operating System : Windows XP
✓ Language : JAVA, J2EE
✓ Front End : JSP, Servlet
✓ Back End : MySQL
✓ Web server : Apache Tomcat
✓ Builder Tool : MyEclipse

5.2 HARDWARE REQUIREMENTS

✓ Main Processor : Pentium IV
✓ Ram : 512 Mb Ram
✓ Mother Board : 845gvm Intel Chipset
✓ Hard Disk : 80GB
✓ Monitor : 17” Color Monitor
✓ Keyboard : Standard 102 Keys
✓ Mouse : Optical mouse
SOFTWARE

REQUIREMENT

SPECIFICATIONS
6. SOFTWARE REQUIREMENT SPECIFICATIONS

6.1 User Interface

Front End:

Front-end is the generalized terms that refers to the initial stages of a process. The front-end is responsible for collecting input in various forms from the user and processing it to conform to a specification the back-end can use. The front-end is a kind of interface between the user and the back-end. The proposed system is platform independent i.e. the application is accessible using a web browser like Internet Explorer, Firefox etc.

Server Side Scripting Language:

Server-side scripting is a web server technology in which a user's request is fulfilled by running a script directly on the web server to generate dynamic web pages. It is usually used to provide interactive web sites that interface to databases or other data stores. Server-side scripting has the ability to highly customize the response based on the user's requirements, access rights, or queries into data stores.

JSP is a widely used general-purpose scripting language that is especially suited for Web development. In our proposed system JSP is the server side scripting language.

Client-side scripting:

Client-side scripting generally refers to the class of computer programs on the web that are executed client-side, by the user's web browser, instead of server-side (on the web server). This type of computer programming is an important part of the Dynamic HTML (DHTML) concept, enabling web pages to be scripted; that is, to have different and changing content depending on user input, environmental conditions (such as the time of day), or other variables.

Back end:

Database Server:
MySQL - MySQL stands for "My Structured Query Language". The program runs as a server providing multi-user access to a number of databases.

MySQL Enterprise Server software is the most reliable, secure and up-to-date version of MySQL for cost-effectively delivering E-commerce, Online Transaction Processing (OLTP), and multi-terabyte Data Warehousing applications.

It is a fully integrated transaction-safe, ACID compliant database with full commit, rollback, and crash recovery and row level locking capabilities.

MySQL delivers the ease of use, scalability, and performance that has made MySQL the world's most popular open source database.

MySQL is the most common language used for accessing a database. It has been in use for many years by many database vendors. Many consider it the best database language to use.

MySQL is a language which consists of a set of commands that we use to create, make changes to, and retrieve data from a database these commands can be issued through a Graphical User Interface or by embedding them in a computer program that we write.

To allow access to the database through web site, we will need to create Common Gateway Interface scripts. These scripts are small computer programs which run on the web hosting server and are activated by clicking on a link or a button in a web page. This will allow users of the web site to interact with the web site in a more meaningful manner.

In MySQL we can create tables to hold the data and loading them with the desired information. Then we can answer different sorts of questions by retrieving data from the tables. We can perform the following operations:

• Create a database

• Create a table

• Load data into the table

• Retrieve data from the table in various ways

• Use multiple tables
DATABASES, which lists the databases managed by the server. To find out which database is currently selected, one should use the DATABASE() function:

mysql> SELECT DATABASE();

+----------+
<table>
<thead>
<tr>
<th>DATABASE()</th>
</tr>
</thead>
<tbody>
<tr>
<td>menagerie</td>
</tr>
<tr>
<td>-----------</td>
</tr>
</tbody>
</table>

If any database not selected, the result is NULL. To find out what tables the default database contains use this command:

mysql> SHOW TABLES;

+---------------------+
<table>
<thead>
<tr>
<th>Tables_in_menagerie</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
</tr>
</tbody>
</table>
+---------------------+

The name of the column in the output produced by this statement is always Tables_in_db_name, where db_name is the name of the database. We can use SHOW TABLES Syntax, for more information.

If we want to find out about the structure of a table, the DESCRIBE command is useful; it displays information about each of a table's columns: for example:

mysql> DESCRIBE person;

+---------------------------------+
<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Null</th>
<th>Key</th>
<th>Default</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>varchar(20)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>fname</td>
<td>varchar(20)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>lname</td>
<td>varchar(20)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
<tr>
<td>address</td>
<td>varchar(1)</td>
<td>YES</td>
<td></td>
<td>NULL</td>
<td></td>
</tr>
</tbody>
</table>

Field indicates the column name, Type is the data type for the column, NULL indicates whether the column can contain NULL values, Key indicates whether the column is indexed, and Default specifies the column's default value. Extra displays special information about columns: If a column was created with the AUTO_INCREMENT option, the value will be auto_increment rather than empty.

DESC is a short form of DESCRIBE. See DESCRIBE Syntax, for more information.

We can obtain the CREATE TABLE statement necessary to create an existing table using the SHOW CREATE TABLE statement with SHOW CREATE TABLE Syntax.

The database is simple, but it is not difficult to think of real-world situations in which a similar type of database might be used. A database containing some of the queries and sample data. MySQL addresses through several statements that provide information about the databases and tables it supports.

### 6.2 SURVEY OF TECHNOLOGIES

The literature survey is a journey of the project right from collecting relevant data to detailed research and study essential for carrying out the project.

**Java**

James Gosling, Patrick Naughton, Chris Warth, Ed Frank and Mike Sheridan convinced Java at Sun Microsystems, Inc. in 1991. It took 18 months to develop the first working version. This language was initially called “Oak” but was renamed “Java” in 1995.
Object oriented programming is the core of Java. All Java Programs are object oriented data. The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple and powerful
- Secure
- Portable
- Object-Oriented
- Robust
- Multithreaded
- Architecture-neutral
- Interpreted
- High performance
- Distributed and Dynamic.

With the emergence of World Wide Web, java was propelled to the forefront of the computer language design, because the web demanded portable programs. Java is programmers language it is logically consistent. Java is not a language with training wheels. It is language for professional programmers.

**JSP: Java Server Pages**

JSP is a widely used general-purpose scripting language that is especially suited for Web development. In our proposed system JSP is the server side scripting language.

Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. JSP provide excellent server side scripting support for creating database driven web applications. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy. JSP pages are efficient, it loads into the web servers
Main reasons to use JSP:

- Multi platform.
- Component reuse by using Javabeans and EJB.
- Advantages of Java.

We can take one JSP file and move it to another platform, web server or JSP Servlet engine.

In today's environment most web sites servers dynamic pages based on user request. Database is very convenient way to store the data of users and other things. JDBC provide excellent database connectivity in heterogeneous database environment. Using JSP and JDBC its very easy to develop database driven web application.

Java is known for its characteristic of "write once, run anywhere." JSP pages are platform independent. Your port your .jsp pages to any platform.

The most significant of the many good reasons is that it is amazingly easy to develop sophisticated Web sites with JSPs. Through a mechanism called JavaBeans, JSPs have made it possible for large teams or individuals working on complex projects to divide the work in such a
way as to make each piece simple and manageable, without sacrificing any power. JSPs also provide a great deal of flexibility when generating HTML, through the ability to create HTML-like custom tags.

JSPs are compiled into Java Servlets by a JSP compiler. A JSP compiler may generate a servlet in Java code that is then compiled by the Java compiler, or it may generate byte code for the servlet directly. "Java Server Pages" is a technology released by Sun.

In addition to this fundamental ease of development, high-quality JSP tools are readily available and easy to use. There is no need to buy expensive software or commit to a particular operating system in order to use JSPs.

JSP provides a Tag based approach to develop the server side executable application which is used to generate dynamic content.

There are five main tags:

1. Declaration tag
2. Expression tag
3. Directive tag
4. Scriptlet tag
5. Action tag

**Declaration tag** ( `<%! %>` )

This tag allows the developer to declare variables or methods.

Before the declaration it must have `<%!

At the end of the declaration, the developer must have `%>

Code placed in this tag must end in a semicolon ( ; ).

**Expression tag** ( `<%= %>` )

This tag allows the developer to embed any java expression and is short for `out.println()`.
A semicolon ( ;) does not appear at the end of the code inside the tag.

**Directive tag** ( `<% @ directive ... %>` )

A JSP directive gives special information about the page to the JSP Engine. There are three main types of directives:

1) page - processing information for this page.
2) Include - files to be included.
3) Tag library - tag library to be used in this page.

**Action tag**

There are three main roles of action tags:

1) enable the use of server side Javabeans
2) transfer control between pages
3) browser independent support for applets.

**Scriptlet tag** ( `<% ... %>` )

Between `<%` and `%>` tags, any valid Java code is called a Scriptlet. This code can access any variable or bean declared.

Problems with Servlet – If we want to generate a page, which consists of some dynamic content, then we have to include the entire static content into the Servlet (i.e, out.println method) along with the dynamic content. i.e. when a huge view has to be generated then there was a problem with the application development and modifications(view/application).

While developing web applications using JSP technology we can separate the business logic from the presentation logic. Separation of presentation logic from business logic helps in reducing the time required to manage the project in future. Thus the advantage of JSP is that it provides a better mechanism to develop and maintain huge view compare to servlets.
J2EE :
Short for Java 2 Platform Enterprise Edition. J2EE is a platform-independent, Java-centric environment from Sun for developing, building and deploying Web-based enterprise applications online. The J2EE platform consists of a set of services, APIs, and protocols that provide the functionality for developing multitiered, Web-based applications.

The Java 2 Platform, Enterprise Edition (J2EE) is a set of coordinated specifications and practices that together enable solutions for developing, deploying, and managing multi-tier server-centric applications.

Some of the key features and services of J2EE:

- At the client tier, J2EE supports pure HTML, as well as Java applets or applications. It relies on Java Server Pages and servlet code to create HTML or other formatted data for the client.
- Java Database Connectivity (JDBC), which is the Java equivalent to ODBC, is the standard interface for Java databases.
- The Java servlet API enhances consistency for developers without requiring a graphical user interface.

Servlets :
A servlet is a Java technology based web component, managed by a container, that generates dynamic content. Like other Java-based components, servlets are platform independent Java classes that are compiled to platform neutral bytecode that can be loaded dynamically into and run by a Java enabled web server.

Servlets are generic extensions to the Java enabled. A Servlets dynamically loaded module that services requests from a web server. It runs entirely inside the Java Virtual Machine. There are two types of Servlets:

1. Generic Servlets
2. HTTP Servlets
The HTTP Servlets class extends from the Generic Servlets class. The javax.servlet.http contains the generic interfaces and classes that are implemented and extended by all the Servlets, the javax.servlets.http contains classes that are executed when creating HTTP specific Servlets.

A servlet is managed through a well defined life cycle that defines how it is loaded, instantiated and initialized, handles requests from clients, and how it is taken out of service. This life cycle is expressed in the API by the init, service, and destroy methods of the javax.servlet.Servlet interface.

It has 3 important methods

- init()
- service()
- destroy()

Java Servlets do not have a main() method; hence all Servlets must implements the javax.servlet.Servlet interface. Every time a server receives those points to a servlet, it calls the Servlets.service() method.

Two objects that the service method receives are ServletRequest and ServletResponse. The ServletRequest objects holds the information that is being on the servlet whereas the ServletResponse object is where you place the data you want to send back to the client. When a HTTP Servlet.service() method is invoked, it reads the method type stored in the request and determines which method to invoke on it value.

MyEclipse

MyEclipse Enterprise Workbench is a full-featured, Enterprise class platform and tool suite for developing software applications and systems supporting the full life-cycle of application development. Facilities and features usually found only in high-priced, Enterprise class product are included in MyEclipse. Based on the open industry standards and the Eclipse platform, MyEclipse redefines software pricing, support and delivery release cycles by providing a complete applications development environment for J2EE WEB, XML, UML and databases and the most comprehensive array of application server connectors(25 target environments) to optimize development, testing and portability.

The first commercial J2EE IDE for Eclipse, MyEclipse was launched in 2003 with a handful of features, and the commitment to deliver a complete and affordable development environment through rapid and iterative releases. MyEclipse offers a tremendous value and challenges the misconception that worldclass development tools have to be expensive. MyEclipse
members have access to the Enterprise Workbench, frequent feature releases and updates, free online support and tutorials.

MyEclipse is the most comprehensive Java EE / J2EE IDE for the open source Eclipse platform, period. Over 300,000 man hours have gone into MyEclipse, insuring both depth and breadth of features. MyEclipse incorporates today’s most innovative open standard technologies to provide a development environment for J2EE, XML, UML and databases and a wide array of application server connectors to streamline development, deployment, testing and portability.

MyEclipse Features include

- Java EE development (JSP, JSF, Struts, JSTL, XML, XSD, Servlets, EJB, app-server deployment/debug)
- Database development (ERD, Database Explorer, SQL, DDL, Data editing, Oracle triggers, procedures, packages, ….)
- RAD development (visual page & web flow design tools, JEE Web-DB app. Automation, customizable templates, ….)
- UML development (round trip support, class, sequence, collaboration, deployment, state, activity)
- POJO development (Spring, EJB, Hibernate, Web services, XDoclet……)
- AJAX / Web 2.0 development (JavaScript / CSS / XML / HTML editing / Debugging, JavaScript console, DOM inspector / editor)
- Rich-clien development (Matisse4MyEclipse Java Swing Visual Designer)

**Web Server**: The primary function of a web server is to deliver web pages and associated content (e.g. images, style sheets, JavaScripts) to clients. A client, commonly a web browser or web crawler, makes a request for a specific resource using HTTP and the server responds with the content of that resource. The resource is typically a real file on the server's secondary memory, but this is not necessarily the case and depends on how the web server is implemented.

While the primary function is to serve content, a full implementation of HTTP also includes a way of receiving content from clients. This feature is used for submitting web forms, including uploading of files.
Many generic web servers also support **server-side scripting** e.g. Apache HTTP Server.

Some of the main features are:

- **A Web Server** is a piece of software that enables a website to be viewed using HTTP. HTTP (HyperText Transfer Protocol) is the key protocol for the transfer of data on the web. It dishes out web pages in response to requests from a user sitting at a web browser.

- Web servers aren’t limited to serving up static HTML pages; they can also run programs in response to user requests and return the dynamic results to the user’s browser.

- **Apache Web Server** - The Apache HTTP Server Project is a collaborative software development effort aimed at creating a robust, commercial-grade and freely-available source code implementation of an HTTP (Web) server.

**Apache Tomcat**:

Apache Tomcat is an open source software implementation of the **Java Servlet** and **JavaServer Pages** technologies.

Apache Tomcat is a Java servlet engine and Java Server Pages processor which can run standalone or integrated with the Apache Web server to serve specific virtual paths. This is an aspect of the web that Apache’s Tomcat is very good at because Tomcat provides both Java servlet and Java Server Pages (JSP) technologies (in addition to traditional static pages and external CGI programming). The result is that Tomcat is a good choice for use as a web server for many applications.

**Apache Tomcat software requirements** :

1. Java 2 Software Development Kit version 1.2.2 or higher from Sun Microsystems, formerly known as the **Java Development Kit** or JDK.
2. The Apache Tomcat servlet container and JSP environment from the Jakarta Apache site.
3. The latest version of the Apache Web server for Windows binary distribution of the Apache server for versions 1.3.17.
Apache Tomcat is a Web Server that implements Servlet and Java Server Pages specification from Java Software and includes many additional features that make it a useful platform for developing and deploying web applications and web services.

Tomcat will operate under any Java Development Kit (JDK) environment that provides a JDK 1.5 (also known as Java2 Standard Edition or J2SE) or later platform. The developer will need a Java Development Kit; as opposed to a Java Runtime Environment so that Servlet other classes and JSP pages can be complied. Tomcat 4 has been extensively tested with JDK 1.5, which is recommended Tomcat to set up a development environment, organize the source code, and then build and test the application.

**GSM MODEM: GLOBAL SYSTEM FOR MOBILE COMMUNICATION**

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz.

**THE GSM NETWORK**

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS).

**GSM SUBSCRIBER SERVICES**

There are two basic types of services offered through GSM: telephony (also referred to as teleservices) and data (also referred to as bearer services). Telephony services are mainly voice
services that provide subscribers with the complete capability (including necessary terminal equipment) to communicate with other subscribers. Data services provide the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network. In addition to normal telephony and emergency calling, the following subscriber services are supported by GSM:

   SMS, Voice mail, Fax ,Cell Broadcast  etc.

   In the proposed system , the user paying through credit card and then a dynamic password will appear as ‘sms’ in the user’s authorized mobile.

The following subscriber service is by GSM:

   SMS -- Short Message Services

A convenient facility of the GSM network is the short message service. A message consisting of a maximum of 160 alphanumeric characters can be sent to or from a mobile station. This service can be viewed as an advanced form of alphanumeric paging with a number of advantages. If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has reentered the coverage area of the network. This function ensures that the message will be received.

SMS is an area where the modem can be used to provide features like:

   ✓ Pre-stored SMS transmission.

   ✓ These SMS can be transmitted on certain trigger events in an automation system.

   ✓ SMS can also be used in areas where small text information has to be sent. The transmitter can be an automation system or machines like vending machines, collection machines or applications like positioning systems where the navigator keeps on sending SMS at particular time intervals.

   ✓ SMS can be a solution where GSM data call or GPRS services are not available.
CONCEPT AND TECHNIQUE (FOR GENERATING DYNAMIC PASSWORD)
7. Concept and Techniques (for generating dynamic password)

7.1 One Time Password

The simplest and oldest method of entity authentication is the password-based authentication, where the password is something that the claimant knows.

Password-based authentication is of two types:-

1. Fixed password
2. One time password

Need of One Time Password

- One-time password authentication system (OTP) provides authentication for system access (login) and other applications requiring authentication that is secure against passive attacks based on replaying captured reusable passwords.

- One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used at a later time to gain access to the system. One-time password systems are designed to counter this type of attack, called a "replay attack".

Overview

The authentication system described in this document uses a secret pass-phrase to generate a sequence of one-time (single use) passwords. With this system, the user's secret pass-phrase never needs to cross the network at any time such as during authentication or during pass-phrase changes. Thus, it is not vulnerable to replay attacks. Added security is provided by the property that no secret information need be stored on any system, including the server being protected.

The OTP system protects against external passive attacks against the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information and does not provide protection against either "social engineering" or active attacks.

Introduction

There are two entities in the operation of the OTP one-time password system. The generator must produce the appropriate one-time password from the user's secret pass-phrase and from information provided in the challenge from the server. The server must send a challenge that includes the appropriate generation parameters to the generator, must verify the one-time password received and must store the corresponding one-time password. The server must also facilitate the changing of the user's secret pass-phrase in a secure manner.
SECURE HASH FUNCTION

The security of the OTP system is based on the non-invertability of a secure hash function. Such a function must be tractable to compute in the forward direction, but computationally infeasible to invert.

The interfaces are currently defined for three such hash algorithms, **MD4 and MD5 by Ronald Rivest, and SHA by NIST**. Clearly, the generator and server must use the same algorithm in order to interoperate.

The secure hash algorithms listed above have the property that they accept an input that is arbitrarily long and produce a fixed size output. This is believed to be long enough to be secure and short enough to be entered manually when necessary.

VERIFICATION OF ONE-TIME PASSWORDS

The server system has a database containing, for each user, the one-time password from the successful authentication or the first OTP of a newly initialized sequence. To authenticate the user, the server matches the one-time password entered by the customer. If it matches with the stored OTP in db, the authentication is successful.

7.2 MD5

Overview

This document describes the MD5 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly.

The MD5 algorithm is an extension of the MD4 message-digest algorithm. MD5 is slightly slower than MD4, but is more "conservative" in design. MD5 was designed because it was felt that MD4 was perhaps being adopted for use more quickly than justified by the existing critical review; because MD4 was designed to be exceptionally fast, it is "at the edge" in terms of risking successful cryptanalytic attack. MD5 backs off a bit, giving up a little in speed for a much greater likelihood of ultimate security. It incorporates some suggestions made by various reviewers, and contains additional optimizations. The MD5 algorithm is being placed in the public domain for review and possible adoption as a standard.
MD5 Algorithm Description

The following five steps are performed to compute the message digest of the message:–

Step 1. Append Padding Bits
  - The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512.
  - Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended.

Step 2. Append Length
  - A 64-bit representation of b (the length of the message before the padding bits were added) is appended to the result of the previous step. In the unlikely event that b is greater than $2^{64}$, then only the low-order 64 bits of b are used.

Step 3. Initialize MD Buffer
  - A four-word buffer (A,B,C,D) is used to compute the message digest.
  - Here each of A, B, C, D is a 32-bit register.
  - These registers are initialized to the following values in hexadecimal, low-order bytes first):

  \[
  \begin{align*}
  \text{word } A & : 01 \ 23 \ 45 \ 67 \\
  \text{word } B & : 89 \ ab \ cd \ ef \\
  \text{word } C & : fe \ dc \ ba \ 98 \\
  \text{word } D & : 76 \ 54 \ 32 \ 10
  \end{align*}
  \]

  - The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D.
These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state.

- The processing of a message block consists of four similar stages, termed **rounds**; each round is composed of 16 similar operations based on a non-linear function $F$, modular addition, and left rotation.

![Diagram](image-url)

**Figure 1.** One MDS operation. MDS consists of 64 of these operations, grouped in four rounds of 16 operations. $F$ is a nonlinear function; one function is used in each round. $M_i$ denotes a 32-bit block of the message input, and $K_j$ denotes a 32-bit constant, different for each operation. $<<<_s$ denotes a left bit rotation by $s$ places; $s$ varies for each operation. $+\mod 2^{32}$ denotes addition modulo $2^{32}$. 
Figure illustrates one operation within a round. There are four possible functions $F$; a different one is used in each round:

$F(X, Y, Z) = (X \land Y) \lor (\neg X \land Z)$
$G(X, Y, Z) = (X \land Z) \lor (Y \land \neg Z)$
$H(X, Y, Z) = X \oplus Y \oplus Z$
$I(X, Y, Z) = Y \oplus (X \lor \neg Z)$

$\oplus, \land, \lor, \neg$ denote the XOR, AND, OR and NOT operations respectively.

**Table T, constructed from the sine function**

This step uses a 64-element table $T[1 \ldots 64]$ constructed from the sine function. Let $T[i]$ denote the $i$-th element of the table, which is equal to the integer part of $4294967296 \times \text{abs}(\sin(i))$, where $i$ is in radians. The elements of the table are given in the following slide.
Step 5. Output

- The message digest produced as output is A, B, C, D.
- That is, we begin with the low-order byte of A, and end with the high-order byte of D.
SOFTWARE ENGINEERING PARADIGM APPLIED
8. SOFTWARE ENGINEERING PARADIGM APPLIED

The software engineering paradigm followed is Object-Oriented. When analyzing a problem from an Object-Oriented point of view, the first things that are usually identified are actors and use cases. In this system once we have identified the system environment following the object oriented paradigm was the best way to develop the system as all the processes in the system are concentrated on the actors in the system.

The features of Object oriented paradigm like inheritance and polymorphism make it best suited for the proposed system because if any changes have to be made to this system it is easy as the property of inheritance provides both code and concept reuse. It enhances robustness and gives consistency to the interface.

Methods, Tools and Techniques

The methods, tools, and techniques that shall be used for the System are explained below:

Software process model: Waterfall model

Software programming language: JSP

Software design methodology: Object-oriented analysis & design technique

To store and retrieve information: MySQL


Standard for software project management plan documentation: IEEE Std. 1058-1998 [1]

8.1 Waterfall Model

The **waterfall model** is a sequential software development process, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of Conception, Initiation, Analysis, Design (validation), Construction, Testing and maintenance.

In Waterfall model, the following phases are followed in order:

1. Requirements
2. Analysis
3. System and software Design
4. Testing
5. Coding
6. Maintenance /Acceptation

The waterfall model (Systems Development Life Cycle)
To follow the waterfall model, one proceeds from one phase to the next in a purely sequential manner. For example, one first completes requirements specifications, which are set in stone. When the requirements are fully completed, one proceeds to design. The software is designed and a blueprint is drawn for implementers to follow, the design should be a plan for implementing the requirements given. When the design is fully completed, an implementation of that design is made by coders. Towards the later stages of this implementation phase, separate software components produced are combined to introduce new functionality and reduced risk through the removal of errors.

1. **Requirements Analysis & Definition:** All possible requirements of the system to be developed are captured in this phase. Requirements are set of functionalities and constraints that the end-user (who will be using the system) expects from the system. The requirements are gathered from the end-user by consultation, these requirements are analyzed for their validity and the possibility of incorporating the requirements in the system to be development is also studied.

2. **System & Software Design:** Before a starting for actual coding, it is highly important to understand what we are going to create and what it should look like? The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model.

3. **Coding:** On receiving system design documents, the work is divided in modules/units and actual coding is started. The system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality; this is referred to as Unit Testing. Unit testing mainly verifies if the modules/units meet their specifications and then the coding started.
4. **Integration & System Testing**: The system is first divided in units which are developed and tested for their functionalities. These units are integrated into a complete system during Integration phase and tested to check if all modules/units coordinate between each other and the system as a whole behaves as per the specifications. After successfully testing of the software, it is delivered to the customer.

5. **Acceptance & Maintenance**: This phase of "The Waterfall Model" is virtually never ending phase (Very long). Generally, problems with the system developed (which are not found during the development life cycle) come up after its practical use starts, so the issues related to the system are solved after deployment of the system. Not all the problems come in picture directly but they arise time to time and needs to be solved; hence this process is referred as Maintenance.

Thus the waterfall model maintains that one should move to a phase only when its preceding phase is completed and perfected.

The waterfall model has many attractive features:

- Clearly defined deliverables at the end of each phase, so that the client can take decisions on continuing the project.
- Incremental resource commitment. The client does not have to make a full commitment on the project at the beginning.
- Isolation of the problem early in the process.

The figure in next page provides an illustration for the above description:
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

Systems Development Life Cycle (SDLC)

User

Request

Problem definition

Problem statement

Feasibility study

Feasibility report

System analysis

Specs of existing system

System Design

Specs of proposed system

System construction

Proposed system

System testing & evaluation

User needs
ANALYSIS
AND DESIGN
9. ANALYSIS AND DESIGN

- **Cardholder**: User using credit/debit card.
- **Merchant**: Retailer that accepts credit/debit cards.
- **Issuer**: It authorizes the person to use card for transaction.
- **Acquirer**: Those who supports merchant by providing services for processing card transaction.
- **Gateways**: An interface that links the internet shopper, online merchant and secure processing system in a secure environment.

Entities:

In the proposed system **Merchant** is taken as **an Online Book Shop**.

The Book Shop contain:

- ✓ Customer details
- ✓ Books category
- ✓ Books Id
- ✓ Price
- ✓ Amount
- ✓ Payment option

SPS.Trans is the service provider for secure transaction. It contains:

- ♦ Merchant: Online Book shop details.
- ♦ Credit card details of registered cardholder.
- ♦ Password details.
9.1 USE CASE DIAGRAM

New User

- Login
- Shops online

- Merchant Admin
  - choose payment mode
  - Check details
  - Verify credit card pin

Existing User

- get password
- provide password
- view transaction

Note: 1) New user means who is logging into the system, 2) existing user means who has logged into the system.
9.2 Entity Relationship Diagram

Following diagram explains the Entity Relationship of the proposed system.
9.3 DATA FLOW DIAGRAM

In the Normal convention, Logical DFD can be completed using only four notations.

**Data flow diagram notation:**

**External Entities/Terminators:** are outside of the system being modeled. Terminators represent where information comes from and where it goes. In designing a system, we have no idea about what these terminators do or how they do it.

**Processes:** modify the inputs in the process of generating the outputs.

**Data Stores:** represent a place in the process where data comes to rest. A DFD does not say anything about the relative timing of the processes, so a data store might be a place to accumulate data over a year for the annual accounting process.

**Data Flows:** are how data moves between terminators, processes, and data stores (those that cross the system boundary are known as IO or Input Output Descriptions).

The Symbols can be diagrammatically represented as follows:-

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rectangle:</strong></td>
<td>Represents a data source or destination.</td>
</tr>
<tr>
<td><strong>Directed Line:</strong></td>
<td>Represents the flow of data that is a data stream.</td>
</tr>
<tr>
<td><strong>Bubble:</strong></td>
<td>Represents a process that performs data streams.</td>
</tr>
<tr>
<td><strong>Open-Ended Rectangle</strong></td>
<td>Represents data storage.</td>
</tr>
</tbody>
</table>
Developing a DFD Event Partitioning Approach:

This approach was described by Edward Yourdon. To construct a detailed DFD, the list of all events is made.

1. For each event a process is constructed.
2. Each process is linked (with incoming data flows) directly with other processes or via data stores, so that it has enough information to respond to given event.
3. The reaction of each process to a given event is modeled by an outgoing data flow.

[Note :- SPS.Trans is the service provider for secure transaction. It contains:

- Merchant : Online Book shop details.
- Credit card details of registered cardholder.
- Password details.]

Level 0 DFD - Context Diagram

User Login : Level 0

Diagram: 
- User login details from User to SPS Management System.
- Output from SPS Management System to User.
- User login to User.
Transaction process: Level 0

User → SPSMS

- Transaction details
- Credit card

SPSMS → Online book Shop

- Confirmation details

User → SPSMS

- Transaction and password
- Confirmation

User
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

Level 1:

- User login
- Validate login
- Authorized
- Locate Online Book shop
- Order
- Check Payment
- Confirm Payment
- SPS
- Produce and send dynamic password
- Transaction Confirmation details
- User
- User register
- User details
- Book table
- Confirm purchase order
- Order details
- Payment
- Verify Card Authentication
- Credit card
User Login: Level 2

User -> User login details -> Validates User exists or not -> User details -> User Register

If user does not exist or password is wrong -> Display appropriate error message -> User

User Login details
User Registration: Level 2

User details
User 

Checks User
Exists or
Registration details

User Register

If User does not exist collects details of...

Add new

User register

Registration confirmation

User
Transacion process: Level 2

1. User
   - Login details
   - Validate Login details
   - User register
   - Authorized user
   - Selected
   - Book details
   - Purchase from
   - Order
   - Confirm Payment
   - Credit card
   - Payment status
   - SPS
   - Password and Transaction
   - User
   - Order
   - Confirm Payment
   - Credit card
   - Payment status
   - SPS
   - User
SYSTEM DESIGN
10 SYSTEM DESIGN

10.1 DIFFERENT DESIGN:

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements.

Logical design

The logical design of a system pertains to an abstract representation of the data flows, inputs and outputs of the system. This is often conducted via modelling, using an over-abstract (and sometimes graphical) model of the actual system. In the context of systems design, modelling can undertake the following forms, including

Physical design

The physical design relates to the actual input and output processes of the system. This is laid down in terms of how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed as output.

Physical design, in this context, does not refer to the tangible physical design of an information system. To use an analogy, a personal computer's physical design involves input via a keyboard, processing within the CPU, and output via a monitor, printer, etc. It would not concern the actual layout of the tangible hardware, which for a PC would be a monitor, CPU, motherboard, hard drive, modems, video/graphics cards, USB slots, etc.

Alternative design methodologies

Rapid application development (RAD)

Rapid application development (RAD) is a methodology in which a systems designer produces prototypes for an end-user. The end-user reviews the prototype, and offers feedback on its suitability. This process is repeated until the end-user is satisfied with the final system.
Joint application design (JAD)

Joint application design (JAD) is a methodology which evolved from RAD, in which a systems designer consults with a group consisting of the following parties:

- Executive sponsor
- Systems Designer
- Managers of the system

JAD involves a number of stages, in which the group collectively develops an agreed pattern for the design and implementation of the system.

10.2 DATABASE DESIGN

Data Design

A well-designed database is essential for the performance of the system. Several tables are manipulated for varying purposes.

Name of the table: Credit card database as provided by bank.

Purpose: Contains user credit card details.

1. Credit_card table

<table>
<thead>
<tr>
<th>SI No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Creditcardnumber</td>
<td>Varchar</td>
<td>30</td>
<td>Primary Key</td>
<td>The unique number of the card</td>
</tr>
<tr>
<td>2</td>
<td>Month</td>
<td>Varchar</td>
<td>30</td>
<td>null</td>
<td>Show Month</td>
</tr>
<tr>
<td>3</td>
<td>Year</td>
<td>Varchar</td>
<td>10</td>
<td>null</td>
<td>Show Year</td>
</tr>
<tr>
<td>4</td>
<td>Token</td>
<td>Varchar</td>
<td>10</td>
<td>null</td>
<td>Generated Password</td>
</tr>
<tr>
<td>5</td>
<td>Pinnumber</td>
<td>Varchar</td>
<td>30</td>
<td>null</td>
<td>Unique pin number</td>
</tr>
<tr>
<td>6</td>
<td>Phonenumber</td>
<td>Varchar</td>
<td>30</td>
<td>null</td>
<td>User mobile number</td>
</tr>
</tbody>
</table>
In the following database introducing a online book shop from where the user will purchase the book and start its credit card payment in further steps.

Name of the table: Customers Tables

Purpose: The details of the customer is stored in this table.

2. Customers Tables

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>username</td>
<td>Varchar</td>
<td>(50)</td>
<td>Primary key</td>
<td>Unique name given by the user</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>varchar</td>
<td>(50)</td>
<td>not null</td>
<td>Password of the user</td>
</tr>
<tr>
<td>3</td>
<td>firstname</td>
<td>varchar</td>
<td>(50)</td>
<td>null</td>
<td>User first name</td>
</tr>
<tr>
<td>4</td>
<td>lastname</td>
<td>varchar</td>
<td>(50)</td>
<td>null</td>
<td>User last name</td>
</tr>
<tr>
<td>5</td>
<td>address</td>
<td>varchar</td>
<td>(100)</td>
<td>null</td>
<td>The address of user</td>
</tr>
<tr>
<td>7</td>
<td>state</td>
<td>varchar</td>
<td>(100)</td>
<td>null</td>
<td>Name of the state</td>
</tr>
<tr>
<td>8</td>
<td>pincode</td>
<td>varchar</td>
<td>(20)</td>
<td>null</td>
<td>The code detail</td>
</tr>
<tr>
<td>9</td>
<td>telephone</td>
<td>varchar</td>
<td>(20)</td>
<td>null</td>
<td>The contact number</td>
</tr>
</tbody>
</table>
Name of the table: Cart table
Purpose: To show the online transaction: First introduce an online book shop from where the user can check to purchase a book.

3. Book_Cart Table

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BookId</td>
<td>Varchar</td>
<td>30</td>
<td>Primary key</td>
<td>The unique id of the book</td>
</tr>
<tr>
<td>2</td>
<td>BookName</td>
<td>Varchar</td>
<td>100</td>
<td>null</td>
<td>Name of the book</td>
</tr>
<tr>
<td>3</td>
<td>Price</td>
<td>Double</td>
<td></td>
<td>null</td>
<td>Price of the book</td>
</tr>
<tr>
<td>4</td>
<td>Quantity</td>
<td>Int</td>
<td>11</td>
<td>null</td>
<td>Number of books</td>
</tr>
<tr>
<td>5</td>
<td>SessionId</td>
<td>Varchar</td>
<td>200</td>
<td>null</td>
<td>The session id.</td>
</tr>
</tbody>
</table>

Name of the table: Categories table
Purpose: The details of the categories offered by the book shop are stored in this table.

4. Categories Tables

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Category_Id</td>
<td>Int</td>
<td>10</td>
<td>Primary Key</td>
<td>Unique id</td>
</tr>
<tr>
<td>2</td>
<td>Category_Name</td>
<td>Varchar</td>
<td>200</td>
<td>null</td>
<td>Name of category</td>
</tr>
</tbody>
</table>
Name of the table: Book
Purpose: Individual book details are stored in this table.

5. Books Table

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>isbn</td>
<td>varchar</td>
<td>100</td>
<td>Primary key</td>
<td>Unique code</td>
</tr>
<tr>
<td>2</td>
<td>title</td>
<td>varchar</td>
<td>300</td>
<td>Null</td>
<td>Title of the book</td>
</tr>
<tr>
<td>3</td>
<td>subtitle</td>
<td>varchar</td>
<td>300</td>
<td>Null</td>
<td>Subtitle of the book</td>
</tr>
<tr>
<td>4</td>
<td>author</td>
<td>varchar</td>
<td>300</td>
<td>Null</td>
<td>The name of author</td>
</tr>
<tr>
<td>5</td>
<td>publisheddate</td>
<td>varchar</td>
<td>200</td>
<td>Null</td>
<td>Date of publication</td>
</tr>
<tr>
<td>6</td>
<td>pages</td>
<td>Int</td>
<td>300</td>
<td>Null</td>
<td>Number of pages</td>
</tr>
<tr>
<td>7</td>
<td>category</td>
<td>Int</td>
<td>10</td>
<td>Null</td>
<td>Category of the book</td>
</tr>
<tr>
<td>8</td>
<td>newrelease</td>
<td>Int</td>
<td>10</td>
<td>Null</td>
<td>Any new release</td>
</tr>
<tr>
<td>9</td>
<td>detail</td>
<td>varchar</td>
<td>200</td>
<td>Null</td>
<td>Other details</td>
</tr>
<tr>
<td>10</td>
<td>price</td>
<td>double</td>
<td></td>
<td>Null</td>
<td>The cost of the book</td>
</tr>
</tbody>
</table>

Name of the table: Order Items Table
Purpose: All details of the item with its order such as order quantity, orderid are stored in this table.

6. Order_Items Table

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Field Name</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>orderid</td>
<td>Int</td>
<td>12</td>
<td>Foreign key</td>
<td>The orderid</td>
</tr>
<tr>
<td>2</td>
<td>bookid</td>
<td>varchar</td>
<td>50</td>
<td>Primary Key</td>
<td>The unique bookid of the ordered book</td>
</tr>
<tr>
<td>3</td>
<td>quantity</td>
<td>Int</td>
<td>12</td>
<td>null</td>
<td>Number of books</td>
</tr>
</tbody>
</table>
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

<table>
<thead>
<tr>
<th>Sl No</th>
<th>FieldName</th>
<th>Type</th>
<th>Width</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>orderid</td>
<td>Int</td>
<td>12</td>
<td>Primary key</td>
<td>The unique orderid</td>
</tr>
<tr>
<td>2</td>
<td>amount</td>
<td>double</td>
<td></td>
<td>Null</td>
<td>The amount (if any)</td>
</tr>
<tr>
<td>3</td>
<td>orderdate</td>
<td>varchar</td>
<td>100</td>
<td>Null</td>
<td>Date of the order placed</td>
</tr>
<tr>
<td>4</td>
<td>customername</td>
<td>varchar</td>
<td>100</td>
<td>null</td>
<td>The name of the customer</td>
</tr>
</tbody>
</table>

Name of the table : Orders Table

Purpose : The details of order from customer such as order date, amount are stored in this table.

7. Orders Table

10.3 Modular Design

There are mainly five modules in the system:-

- **User Interaction Design**
  
  Developing the Graphical User Interface of View Layer in Java Server Pages for customers to login and select the items to purchase in web with Java Script Technology.

- **Server Validation and Process**
  
  Implementing the Model Layer of getting the inputs from the View Layer and processing of the Validation of Data logically in servlet Technology and forwarding the Response to Tomcat server in turn Display the corresponding view Page.

- **Database Interaction**
Connecting the Database Driver used with Control Layer to validate the Request received from the Tomcat server and Responding the further process and is implemented Globalized such that the Database can be changed easily in code.

- **Generating OTP Algorithm**

  The card no and pin no from the view layer and Current Day ,Date and time are take from the packages and implemented as parameter for the OTP Algorithm. As a Result it will generate the Dynamic Password

- **GSM Modem Implementation**

  and connecting the Modem to the PC with serial port. GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. Importing the comm Driver

In the proposed system there are folloeing users:-

- **Cardholder** : User using credit/debit card.
- **Merchant** : Retailer that accepts credit/debit cards.
- **Issuer** : It authorizes the person to use card for transaction.
- **Acquirer** : Those who supports merchant by providing services for processing card transaction.
- **Gateways** : An interface that links the internet shopper, online merchant and secure processing system in a secure environment.

Entities:

In the proposed system Merchant is taken as -- **an Online Book Shop**.

The Book Shop contain :

- ✓ Customer details
SPS.Trans is the service provider for secure transaction. It contains:

- Merchant: Online Book shop details.
- Credit card details of registered cardholder.
- Password details.
TESTINGS
11. TESTING

Software testing is an empirical investigation conducted to provide stakeholders with information about the quality of the product or service under test, with respect to the context in which it is intended to operate. Software Testing also provides an objective, independent view of the software to allow the business to appreciate and understand the risks at implementation of the software. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs.

11.1 Testing techniques and Testing strategies:

There are four testing strategies that are mainly used. These are,

- Unit Testing
- Integration Testing
- Validation Testing
- System Testing

This system was tested using Unit Testing and Integration Testing strategies because these were the most relevant approaches for this project.

Software Testing Techniques:

Specification-based testing: Specification-based testing aims to test the functionality of software according to the applicable requirements. Thus, the tester inputs data into, and only sees the output from, the test object. This level of testing usually requires thorough test cases to be provided to the tester, who then can simply verify that for a given input, the output value (or behavior), either "is" or "is not" the same as the expected value specified in the test case. Specification-based testing is necessary, but it is insufficient to guard against certain risks.

A software engineering product can be tested in one of the two ways:
Black Box Testing:

Knowing a specified function that a product has been designed to perform, determine whether each function is fully operational. Black box testing treats the software as a "black box"—without any knowledge of internal implementation. Black box testing methods include: equivalence partitioning, boundary value analysis, all-pairs testing, fuzz testing, model-based testing, traceability matrix, exploratory testing and specification-based testing. Tests are based on requirements and functionality.

White Box Testing:

Knowing the internal workings of a software product determine whether the internal operations implementing the functions performs according to the specification, and all the internal components have been adequately exercised.

The following types of white box testing exist:

- API testing (application programming interface) - Testing of the application using Public and Private APIs
- Code coverage - creating tests to satisfy some criteria of code coverage (e.g., the test designer can create tests to cause all statements in the program to be executed at least once)
- Fault injection methods - improving the coverage of a test by introducing faults to test code paths
- Mutation testing methods
- Static testing - White box testing includes all static testing

Unit testing:
We adopt white box testing when using this testing technique. This testing was carried out on individual components of the software that were designed. Each individual module was tested using this technique during the coding phase. Every component was checked to make sure that they adhere strictly to the specifications spelt out in the Data Flow Diagram and ensure that they perform the purpose intended for them.

All the names of the variables are scrutinized to make sure that they truly reflect the element they represent. All the looping mechanisms were verified to ensure that they were as decided. Besides these, we trace through the code manually to capture syntax errors and logical errors.

**Integration Testing:**

After finishing the Unit Testing, next is the integration testing process. In this testing process we put our focus on identifying the interfaces between components and their functionality as dictated in the Data Flow Diagram. The Bottom Up incremental approach was adopted during these testing. Low-level modules are integrated and combined as a cluster before testing.

The Black Box testing technique was employed here. The interfaces between the components were tested first. This allowed identifying any wrong linkages or parameters passing early in the development process as it can be just passed in a set of data and checked if the result returned is an accepted one.

**Validation Testing:**

Software testing and validation is achieved through a series of black box test cases. A test procedure defines specific test cases that demonstrate conformity with the requirements. Both, the plan the procedure are designed to ensure that all functional requirements are achieved, documentation is correct and other requirements are met. After each validation test case has been conducted, one of the two possible conditions exists. They are,

- The function or performance characteristics confirm to specification and are accepted.
- A deviation from the specification is uncovered and a deficiency list is created.
The deviation or error discovered at this stage in project can rarely be corrected prior to scheduled completion. It is necessary to negotiate with the customer to establish a method of resolving deficiencies.

**System Testing**

System testing is a series of different tests whose primary purpose is to fully exercise the computer-based system. Although each test has a different purpose, all the work should verify that all system elements have been properly integrated and perform integrated functions.

System testing also ensures that the project works well in the environment. It traps the errors and allows convenient processing of errors without coming out of the program abruptly.

Recovery testing is done in such a way that failure is forced to a software system and checked whether the recovery is proper and accurate. The performance of system is highly effective.

**Web Testing**

Our proposed project is of 3 tier applications (developed for Internet). Here we will be having Browser, web server and DB server. The applications accessible in browser would be developed in HTML, JavaScript etc. We can monitor through these applications for the web server would be developed in Java, JSP, JavaScript, (All the manipulations are done on the web server with the help of these programs developed). The DB server would be having oracle, sql server, sybase, mysql etc. (All data is stored in the database available on the DB server).

**The tests performed on these types of applications would be**
- User interface testing
- Functionality testing
- Security testing
- Browser compatibility testing
- Load / stress testing
- Storage and data volume testing
A web-application is a three-tier application.

This has a browser (monitors data) [monitoring is done using html-> webserver (manipulates data) [manipulations are done using programming languages or scripts like adv java,jsp, javascript,] -> database server (stores data) [data storage and retrieval is done using databases like mysql].

The types of tests, which can be applied on this type of applications, are:
1. User interface testing for validation & user friendliness
2. Functionality testing to validate behaviors, i/p, error handling, o/p, manipulations, services levels, order of functionality, links, content of web page & backend coverage’s
3. Security testing
4. Browser compatibility
5. Load / stress testing
6. Interoperability testing
7. Storage & data volume testing

11.2 Testing with different test cases:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Test case No</th>
<th>Test Case Name</th>
<th>Test Step No</th>
<th>Description</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TC 1_Login</td>
<td>To check whether the user is able to login with the valid user id and pwd</td>
<td>Step 1</td>
<td>Type the URL in the IE and click on GO button</td>
<td>The Login page should be displayed.</td>
</tr>
<tr>
<td></td>
<td>screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 2</td>
<td>Enter the valid username and pwd in the USER NAME field and PASSWORD field.</td>
<td>The fields should accept the data entered by the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 3</td>
<td>Click on the OK button.</td>
<td>The User should be taken to the SPS homepage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>TC 2_Login screen</td>
<td>To check whether the user is not able to login to the SPS with the valid user id and invalid pwd</td>
<td>Step 1</td>
<td>Type the URL in the IE and click on GO button</td>
<td>The SPS Login page should be displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 2</td>
<td>Enter the valid username and invalid pwd in the USER NAME field and PASSWORD field.</td>
<td>The fields should accept the data entered by the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 3</td>
<td>Click on the OK button.</td>
<td>The Error message 'Login Failed' should be displayed.</td>
</tr>
<tr>
<td>3</td>
<td>TC 3_Login screen</td>
<td>To check whether the user is not able to login to the with the invalid user id and valid pwd</td>
<td>Step 1</td>
<td>Type the URL in the IE and click on GO button</td>
<td>The Login page should be displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 2</td>
<td>Enter the invalid username and valid pwd in the USER NAME field and PASSWORD field.</td>
<td>The fields should accept the data entered by the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Step 3</td>
<td>Click on the OK button.</td>
<td>The Error message 'Login Failed' should be displayed.</td>
</tr>
<tr>
<td>4</td>
<td>TC 4_Login screen</td>
<td>To check whether the user is not able to login to the</td>
<td>Step 1</td>
<td>Type the URL in the IE and click on GO button</td>
<td>The Login page should be displayed.</td>
</tr>
<tr>
<td></td>
<td>with the invalid user id and invalid pwd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step 2</td>
<td>Enter the invalid username and valid pwd in the USER NAME field and PASSWORD field.</td>
<td>The fields should accept the data entered by the user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step 3</td>
<td>Click on the OK button.</td>
<td>The Error message 'Login Failed' should be displayed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TC 5_Home page_Sign out function</td>
<td>To check whether the user is able to signout of the application</td>
<td>Step 1</td>
<td>Type the URL in the IE and click on GO button</td>
<td>The Login page should be displayed.</td>
</tr>
</tbody>
</table>
IMPLEMENTATION
12. IMPLEMENTATION

In the implementation phase, the team builds the components either from scratch or by composition. Given the architecture document from the design phase and the requirement document from the analysis phase, the team should build exactly what has been requested, though there is still room for innovation and flexibility. For example, a component may be narrowly designed for this particular system, or the component may be made more general to satisfy a reusability guideline. The architecture document should give guidance. Sometimes, this guidance is found in the requirement document.

The implementation phase deals with issues of quality, performance, baselines, libraries, and debugging. The end deliverable is the product itself. During the implementation phase, the system is built according to the specifications from the previous phases. This includes writing code, performing code reviews, performing tests, selecting components for integration, configuration, and integration.

The implementation includes the following things.

- Careful planning
- Investigation of system and constraints.
- Design the methods to achieve the charge over.
- Training the staff in the changed phase.

Implementation is the state of project where the theoretical design is turned into a working system. The most critical stage in achieving a successful new system is giving the confidence that the new system will work effectively. There are provisions for periodic evaluation of the software after implementation. This process evaluates the system’s performance against predefined requirements. The software used in SPS is platform independent hence implementation is easy. Unlike system
testing, which determines where the system fails so that necessary adjustments can be made, evaluation determines how well the implemented system continues to meet the performance specifications.

MAINTENANCE
13. **MAINTENANCE**
Software maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

The key software maintenance issues are both managerial and technical. Key management issues are: alignment with customer priorities, staffing, which organization does maintenance, estimating costs. Key technical issues are: limited understanding, impact analysis, testing, and maintainability measurement.

Maintenance involves a wide range of activities including correcting, coding, and design errors, updating documentation and test data, and upgrading user support. Maintenance is done after the success implementation. Maintenance is continued till the product is reengineered or deployed to another platform. Maintenance is also done based on fixing the problems reported, changing the interface with other software or hardware enhancing the software.

In this system three types of Maintenances being offered:

- **Corrective Maintenance:** Errors that creep into the system are removed.
- **Adaptive Maintenance:** To Adapt the Changing External Factors.
- **Perfective Maintenance:** To Satisfy the Users.
REPORTS-SCREEN SHOTS
14. REPORTS-SCREEN SHOTS
### TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

#### The Book Store

**Categories**
- C#
- JAVA
- XML

**Customer Login**
- Username: [Field]
- Password: [Field]
- Login
- New User? Register

---

#### The Book Store

**Categories**
- C#
- JAVA
- XML

**Customer Registration**
- Username: [Field] **User name required**
- Password: [Field] ******
- Firstname: pitu
- Lastname: jehwani
- Address1: thane
- Address2: sunshine gali
- City: mumbai
- State: jharkhand
- Postal Code: 814101
- Telephone: [Field] **Telephone No required**
- Register
## Two Factor Authentication Using Mobile-Phone

### The Book Store

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>CUSTOMER REGISTRATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td></td>
</tr>
<tr>
<td>JAVA</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

### Customer Registration Form

- **Username**: raj
- **Password**: ********
- **Firstname**: pihu
- **Lastname**: jethwani
- **Address1**: thane
- **Address2**: sunshine gali
- **City**: mumbai
- **State**: jharkhand
- **Postal Code**: 814101
- **Telephone**: 8807443378

Register Button

### Error Message

Username already exists.
## Two Factor Authentication Using Mobile-Phone

### Customer Registration

<table>
<thead>
<tr>
<th>Username</th>
<th>kavitajethwani</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>******</td>
</tr>
<tr>
<td>Firstname</td>
<td>kavita</td>
</tr>
<tr>
<td>Lastname</td>
<td>jaithwani</td>
</tr>
<tr>
<td>Address1</td>
<td>sunshine gali</td>
</tr>
<tr>
<td>Address2</td>
<td>jharkhanda hostel</td>
</tr>
<tr>
<td>City</td>
<td>dumka</td>
</tr>
<tr>
<td>State</td>
<td>jharkhand</td>
</tr>
<tr>
<td>Postal Code</td>
<td>814101</td>
</tr>
<tr>
<td>Telephone</td>
<td>8907433381</td>
</tr>
</tbody>
</table>

Register

### The Book Store

#### Customer Login

Registration successful, please sign in.

Username: 
Password: 
Login

New User? Register
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE

The Book Store

CATEGORIES
Java
XML

NEW RELEASES
Java I/O, Second Edition
By Elliotte Rusty Harold
Price: Rs. 650.00
All of Java's Input/Output (I/O) facilities are based on streams, which provide simple ways to read and write data of different types. Java I/O, 2nd Edition tells you all you need to know about the four main categories of streams and uncovers less-known features to help make your I/O operations more efficient. You'll also learn how to control number formatting, use characters aside from the standard ASCII character set, and get a head start on writing truly multilingual software. Read more.

Ajax on Java
By Steven Douglas Olson
Price: Rs. 400.00
This practical guide shows you how to make your Java web applications more responsive and dynamic by incorporating new Ajaxian features: suggestion lists, drag-and-drop, and more. Java developers can choose between many different ways of incorporating Ajax, from building JavaScript into your applications "by hand" to using the new Single Page Web Toolkit (GWT). The book includes strategies for integrating Ajax into JSP and JSF applications, and using Ajax with Struts. Read more.

C# 3.0 Design Patterns
By Judith Bishop
Price: Rs. 550.00
Want to speed up the development of your .NET applications? Tackle common programming problems with C# design patterns. This guide explains what design patterns are and why they're used, with tables and guidelines to help you choose one pattern over another, and plenty of case studies to illustrate how each pattern is used in practice. C# 3.0 features are introduced by example and summarized for easy reference. Read more.

The Book Store

CATEGORIES
C#
Java
XML

JAVA I/O, SECOND EDITION

Title: Java I/O, Second Edition
Author: Elliotte Rusty Harold
Published on: May 2006
ISBN: 0321227892
Pages: 726
Price: Rs. 650.00
Add to Cart

Description
All of Java's Input/Output (I/O) facilities are based on streams, which provide simple ways to read and write data of different types. Java provides many different kinds of streams, each with its own application: the universe of streams is divided into four large categories: input streams and output streams; for reading and writing binary data; and readers and writers, for reading and writing textual (character) data. You're almost certainly familiar with the basic kinds of streams—but did you know that there's a CipherOutputStream for reading encrypted data? And a ZipOutputStream for automatically compressing data? Do you know how to use buffered streams effectively to make your I/O operations more efficient? Java I/O, 2nd Edition has been updated for Java 5.0 APIs and tells you all you ever need to know about streams—and probably more.

A discussion of I/O wouldn't be complete without treatment of character sets and formatting. Java supports the Unicode standard, which provides definitions for the character sets of most written languages. Consequently, Java is the first programming language that lets you do I/O in virtually any language. Java also provides a sophisticated model for formatting textual and numeric data. Java I/O, 2nd Edition shows you how to control number formatting.
TWO FACTOR AUTHENTICATION USING MOBILE-PHONE
## The Book Store

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>PAYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td></td>
</tr>
<tr>
<td>JAVA</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

### Order Details

- **Order Id:** 19
- **Total Amount:** Rs. 800.0

### Payment Form

- **Card Type:** MasterCard
- **Card Number:** 1111111111111111
- **Pin:** ****
- **Expiration Date:** 12/20

**Complete Order**

---

## The Book Store

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>ORDER COMPLETED</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td></td>
</tr>
<tr>
<td>JAVA</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

**Secret Key:**

**Login**

**Home**
# Invalid User

# The Book Store

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>ORDER COMPLETED</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td></td>
</tr>
<tr>
<td>JAVA</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

Secret Key: b49de6d5

[LOGIN]

[Home]
<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>ORDER COMPLETED</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#</td>
<td></td>
</tr>
<tr>
<td>JAVA</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

Thank you for purchasing your books from us. Please shop with us again soon!

Home
15. SYSTEM SECURITY MEASURES

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.
Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Integrity

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.
16. Future Scope of the Project

The performance of the system is proved to be efficient. All the Profiles receive an overall benefit through the system. The system provides flexibility for incorporating new features, which may be necessary in future.

In this proposed system, to show the online transaction specifically an example of book shop taken. The SPS system can be equally beneficial for any type of online transaction for example online billing, online reservation, online shopping etc.
Thus the secure processing system is flexible and can be incorporated with new features in the future.

17. CONCLUSION

Two factor authentication system is a user-friendly package and requires little prior knowledge of software. All the suggestions forwarded during the software proposal have been successfully completed and final threshold of application has been crossed. Some errors were spotted out during the system testing and were corrected. The system developed for the given conditions specified by the firm was found working efficiently. The system is highly flexible and is well efficient to make easy interactions with the database. The goal of computer security to maintain the integrity, availability and privacy of information entrusted to the system was successfully obtained.
BIBLIOGRAPHY

Books Referred:

- Hall, Marty, Core Servlets and JavaServer Pages
- JavaScript – David Flanagan
- JavaBeans – Elliotte Rusty Harold
- HTML 4 Unleashed – Rick Darnell.
http://www.learnxpress.com
http://www.developer.com
www.javaworld.com
www.jdbc.postgresql.org
www.jtds.ourceforge.net
www.en.wikipedia.org