DUAL SECURITY ENHANCEMENT PROCESS

PROJECT REPORT

Submitted By

R.V.N.BALAJI

Register No.: 0720300003

in partial fulfillment for the award of the degree

of

MASTER OF COMPUTER APPLICATIONS

in

COMPUTER APPLICATIONS

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution Affiliated to Anna University, Coimbatore)

MAY 2010

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution Affiliated to Anna University, Coimbatore)

COIMBATORE – 641 006.

Department of Computer Applications

PROJECT WORK

MAY 2010

This is to certify that the project entitled

DUAL SECURITY ENHANCEMENT PROCESS

is the bonafide record of project work done by

R.V.N.BALAJI

Register No: 0720300003

of MCA (Computer Applications) during the year 2009-2010.

Veenathan 06/05/10

Project Guide

Head of the Department

Submitted for the Project Viva-Voce examination held on 17-5-2010

17/5/10

Internal Examiner

17/05/2010

External Examiner

DECLARATION

I affirm that the project work titled **DUAL SECURITY ENHANCEMENT PROCESS** being submitted in partial fulfilment for the award of **MASTER OF COMPUTER APPLICATIONS** is the original work carried out by me. It has not formed the part of any other project work submitted for award of any degree or diploma, either in this or any other University.

R.V.N.BALAJI
0720300003

I certify that the declaration made above by the candidate is true

Signature of the Guide,

06/05/10

Ms. R.VEENA SHREE, LECTURER

Contact Us
#13/3,Balaji Complex, 8st Avenue, M.H. Road
Perambur, Chennai,Tamil Nadu 600011
EMail: information@triondata.com
Phone : 044-24963274
www.TriOnData.com

TRI ON DATA

PROJECT COMPLETION CERTIFICATE

We are providing this **Mr.R.V.N.Balaji (Reg. No: 0720300003)** doing Final year MCA in "**KUMARAGURU COLLEGE OF TECHNOLOGY**", for the Project "**Dual security enhancement process**" completed with our extreme Organization.

Project Duration: Dec 2009 to May 2010

The developed software have been tested and forwarded to User Acceptance Testing. After Successful implementation of the Application we are issuing this certificate.

TRI ON DATA,

Prabhu.M
(Team Leader)

ACKNOWLEDGEMENT

First and foremost I thank the Almighty for his continuous blessings showered on me in completing this project successfully.

I wish to express my profound gratitude to **Dr. S.Ramachandran, Principal, Kumaraguru College of Technology, Coimbatore** for providing an opportunity and necessary facilities in carrying out this project work.

I am very glad to extend my deepest thanks to **Dr. A. Muthukumar, Course coordinator, Department of Computer Applications, Kumaraguru College of Technology, Coimbatore,** who has always been a source of inspiration.

I wish to express my unending gratitude to my coordinator **Ms.V. Geetha Asst Professor, Department of Computer Applications** for his unrelenting help, support and advice with regards to my project work. I owe him my profound admiration and respect.

I also take this opportunity to thank my Project guide **Ms. R. Veena Shree, Lecturer, Department of Computer Applications, Kumaraguru College of Technology, Coimbatore** for his continuous support.

I also wish to thank **Mr. Prabhu, Project Manager, Tri On Data, Chennai** for giving me insipiration and support for doing my project.

I wish to thank all my teaching and supporting staff members for their timely help and guidance to complete the project successfully.

CHAPTER NO TABLE OF CONTENTS PAGE NO

ABSTRACT

DUAL SECURITY ENHANCEMENT PROCESS

Web clients and Internet communications pose many security problems not found in traditional client-server applications. Security flaws in web applications easily bypass firewalls and other basic security measures. It's easy to unknowingly write a web application that allows outsiders access to files on the server, gather passwords and customer information, and even alter the application itself despite firewalls and other security you may have implemented.

We're going to focus on application level security system which is the base for the server security. Since the front end accessing level should be maintained very securely to prevent the back end hacking, we're going to build the web application in a secured manner.

We're going to build the web site with the help of various security algorithms which was designed earlier. Though many algorithms are designed for the security purpose, sometimes the advanced security system lacks the feature of the previous one. We've analyzed the security algorithms and finally decided to implement SHA1 algorithm, cryptography and CAPTCHA security system.

We are able to handle the internet and intranet in a secured manner by creation of this web application. Here we are using CAPTCHA security system for internet and SHA1 algorithm for intranet. After deeper analysis of the above specified algorithms, we found that using .NET technology we can easily implement all these concepts with less effort and with ease of use.

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 SYSTEM OVERVIEW

The project titled "**DUAL SECURITY ENHANCEMENT PROCESS**" to build a web site in which a complete dual security system is going to be implemented with an efficient manner.

Dual security which involved a lot of information such as user registration details, captcha secure, encrypt photo and video details, profile information, user details, and moreover the process involved was quite a repetitive one and was prone to numerous errors which could result in inappropriate data being presented to the top management.

This security system deals with the web site access and web site browsing. We analyzed and decided to implement the SHA1 algorithm and CAPTCHA based security system which is more efficient than other security system which is currently in use. So, we're going to build a site for matrimony and this site completely deals like other matrimonial site which is available in the market but here we mainly concentrates on building the security system of the site.

The front end accessing level should be maintained very securely to prevent the back end hacking, we're going to build the web application in a secured manner. We're going to build the web site with the help of various security algorithms which was designed earlier. Though many algorithms are designed for the security purpose, sometimes the advanced security system lacks the feature of the previous one. We've analyzed the security algorithms and finally decided to implement SHA1 algorithm, MD5 cryptography and CAPTCHA security system.

1.2 COMPANY PROFILE

Tri On Data specialized profession on Software Development that helps client organizations identify, evaluate, and developing software executives at various levels. Opportunities on a global scale open up many doors. In a race to encash this, players many a time trip on each other's toes - sometimes cutting corners and making compromises at certain other times.Tri On Data promises to the customer, the complete satisfaction in terms of Quality, Deliverance and Cost optimization and at the same time ensures to the customer the right software have been build and deployed.

Our Approach

Smart application development leverages technology and experience to create an application with a focus on today and an eye on tomorrow.

We work with you to understand your unique needs and requirements and then apply our methodologies, best practices and worldwide resources to help you create a cost-effective and quality application to support your business processes and strategic direction.

TRI ON DATA can provide the full range of application portfolio management support, including project management, program office management, requirements and business case analysis, design, development, quality assurance and performance management. Our strength lies in architecture frameworks and development, managed content services for integrating unstructured content into business processes, and alternative delivery channels like mobility and wireless.

Our Vision

To be recognized as an innovative and customer focused HR Consulting firm empowering our customers with complete HR solutions built on Teamwork, Integrity, Competence and Leadership.

"Converting thoughts into reality". To assist organizations in upgrading the quality of its Human Resources, giving them an edge with our customized software and technical expertise and to be the largest talent management outfit for Indian talent.

Our Mission

To redefine people search by providing innovative, cost effective services to our clients and attain numerous status. Putting technology to the best use and reducing the turnaround time. To plan and build a career for the aspirants in tune with their potential.

Customer Orientation

The secret behind every successful business is the ability of choosing and working with the right partners and right people. Our Clients consider us our partners in progress and this can be mapped in all spheres of quality, services and reliability.

Leadership & Innovation

With customer demanding the best from us at all times; we have evolved our business, our people, our technology and our process to reflect the need of the hour. Our strategy of constant innovation and evolution of our resource, technology and business models have led to a list of very satisfied customers and that is strongly evident through our actions.

Our core values guide every engagement we undertake. These values have been identified based on internal strengths of the organization. They are the guiding parameters for all organization-wide initiatives.

Strategy & Planning

TRI ON DATA provides a broad range of strategy services that are tailored to meet the client's needs. These services are targeted to ensure that our client's evolving business goals can be achieved - now as well as in the future.

CHAPTER 2

SYSTEM STUDY AND ANALYSIS

2.1 PROBLEM STATEMENT

System analysis is the process of gathering and interpreting facts, diagnosing the problems and using the information to recommend improvements on the system. The objectives of the study phase are the establishment of the requirements of the system to be acquired and installed. System analysis or study is a problem solving activity that requires intensive communication between the system users and system developers. The system is studied to the minutest detail and analyzed. . A structured approach has been used in the study phase to identify the needs of the user.

System study includes both a preliminary and detailed stage. During preliminary analysis, the analyst takes quick look at what is required and its costs and benefits justify the perceived need. Detailed analysis include an in depth look at what is needed and cost is more refined.

.

2.2 EXISTING SYSTEM

Attacks against the Cryptography

Sometimes, products even get the cryptography wrong. Some rely on proprietary encryption algorithms. Invariably, these are very weak. Counterpane has had considerable success breaking published encryption algorithms; our track record against proprietary ones is even better. Keeping the algorithm secret isn't much of an impediment to analysis, anyway--it only takes a couple of days to reverse-engineer the cryptographic algorithm from executable code. One system we analyzed, the S/MIME 2 electronic-mail

standard, took a relatively strong design and implemented it with a weak cryptographic algorithm. The system for DVD encryption took a weak algorithm and made it weaker.

We've seen many other cryptographic mistakes: implementations that repeat "unique" random values, digital signature algorithms that don't properly verify parameters, hash functions altered to defeat the very properties they're being used for. We've seen cryptographic protocols used in ways that were not intended by the protocols' designers, and protocols "optimized" in seemingly trivial ways that completely break their security.

Attacks against Passwords

Many systems break because they rely on user-generated passwords. Left to themselves, people don't choose strong passwords. If they're forced to use strong passwords, they can't remember them. If the password becomes a key, it's usually much easier--and faster--to guess the password than it is to brute-force the key; we've seen elaborate security systems fail in this way. Some user interfaces make the problem even worse: limiting the passwords to eight characters, converting everything to lower case, etc. Even passphrases can be weak: searching through 40-character phrases is often much easier than searching through 64-bit random keys. We've also seen key-recovery systems that circumvent strong session keys by using weak passwords for key-recovery.

Attacks against Hardware

Some systems, particularly commerce systems, rely on tamper-resistant hardware for security: smart cards, electronic wallets, dongles, etc. These systems may assume public terminals never fall into the wrong hands, or that those "wrong hands" lack the expertise and equipment to attack the hardware. While hardware security is an important component in many secure systems, we distrust systems whose security rests solely on assumptions about tamper resistance. We've rarely seen tamper resistance techniques that work, and tools for defeating tamper resistance are getting better all the time. When we design systems that use tamper resistance, we always build in complementary security mechanisms just in case the tamper resistance fails.

2.2.1 DRAWBACKS OF THE EXISTING SYSTEM

The drawbacks of the existing system can be summarized as below:

- To take lot of effort to secure the data.
- Many cryptography algorithm repeat the unique random values that don't properly verify the hash code. so the data can easily loss or damage.
- There is no web portal security and the password area very weak algorithm, that algorithm can easily break.

2.3 PROPOSED SYSTEM

Sha1 algorithm provides greatest bond and secure the data from hackers. Captcha provides armed web portal security. Our project provides the resistance over the intruders.

The proposed system will have computerized data entry screens and processes can be carried out based on inputs from those screens. The proposed system has been designed to eliminate the major disadvantage of the existing system.

2.3.1 ADVANTAGES OF THE PROPOSED SYSTEM

The expected benefits of the proposed system are as follows:

- Can protect unauthorized users through captcha and can stop hackers entry from various place.
- Data theft also can protect through captcha and latest sha1 algorithm .
- We can develop the application more and more secure through both captcha and sha1 algorithm.

2.4 FEASIBILITY ANALYSIS

Feasibility analysis is the measure of how beneficial or practical the development of the System will be to the project. Once the problem is explained information is gathered about the system to test whether the system is viable Technically, Financially and Operationally. Thus, feasibility study is carried out in three phases as follows:

2.4.1 TECHNICAL FEASIBILITY

Technical Feasibility is the measure of practicality of a specific technical solution and the availability of technical resources and expertise. It centers on the existing computer system (hardware, software, etc.) and to what extent it can support the new addition. This involves financial consideration to accommodate technical enhancement.

The proposed system is to be developed using ASP.net and SQL SERVER 2000 which are some of the leading technologies in the market. Visual studio .NET 2005 and SQL SERVER 2000 are already available with the company. These technologies work well on Microsoft platforms. When take the project size, it's very small.

2.4.2 ECONOMIC FEASIBILITY

Economic Feasibility is the measure of the cost-effectiveness of the proposed system. The investment to be made in the proposed system must prove a good investment to the project by returning benefits equal to or exceeding the costs incurred in developing the system.

The proposed benefits of the system will outweigh the costs to be incurred during system developed since the system does not require procurement of additional hardware facilities it is economically feasible. It uses ASP.Net and SQL Server 2000 for its development. So it's found that the benefits outweigh costs. .

CHAPTER 3

DEVELOPMENT ENVIRONMENT

3.1 HARDWARE REQUIREMENTS

The hardware support required for deploying the application

Processor	: Intel Pentium IV Processor
Memory	: Minimum 512MB
Hard Disc	: 40GB or More
Monitor	: LG 563A (color)
Mouse	: Logitech
Keyboard	: Logitech

3.2 SOFTWARE REQUIREMENTS

The software support required for deploying the application

Operating System	: Windows XP
Front End Tool	: ASP.NET
Back End Tool	: SQL SERVER 2000
Web Server	: IIS
Markup Language	: HTML

3.3 PROGRAMMING ENVIRONMENT

3.3.1 THE .NET FRAMEWORK

The .NET frame work is a new computing platform that simplifies application development in the highly distributed environment of the internet. To avoid separate runtime environment called the Common Language Runtime (CLR).

OBJECTIVES OF .NET FRAMEWORK

- To provide a consistent Object-oriented programming environment whether object codes is stored and executed locally and internet distributed, or executed remotely.
- To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
- Eliminates the performance problems.
- There are different types of application, such as windows-based application and web-based applications.
- To make communication on distributed environment to ensure that code be accessed by the .NET Framework can integrate with any other code.

COMPONENTS OF .NET FRAMEWORK

THE COMMON LANGUAGE RUN TIME (CLR)

The common language runtime is the foundation of the .NET Framework. It manages code at execution time, providing important services such as memory management, and remoting and also ensures more security and robustness. The concept of code management is a fundamental principle of the runtime code that targets the

runtime is known as managed code, while code that does not target the runtime is known as unmanaged code.

THE .NET FRAMEWORK CLASS LIBRARY

It is a comprehensive, object-oriented collection of reusable type used to develop applications ranging from traditional command-line or graphical user interface (GUI) applications to applications based on the latest innovations provided by ASP.NET, such as Web Forms and XML Web services.

The .NET Frame work can be hosted by unmanaged components that load the common language runtime into their processes and initiate the execution of managed code, there by creating a software environment that can exploit both managed and managed features. The .NET Framework not only provides several runtime hosts, but also supports the development of third-party runtime hosts.

Internet explorer is an example of unmanaged application that hosts the runtime (in the form of a MIME type extensions).using Internet Explorer to hosts the runtime to enables embeds managed components or windows forms controls in HTML documents.

ASP.NET

ASP.NET is the next version of Active Server Pages (ASP); it is a unified web development platform that provides the services for developers to build enterprise-class web applications. While ASP.NET is largely syntax compatible, it also provides a new programming model and infrastructure for more secure, scalable, a stable applications.

ASP.NET is a compiled, NET-based environment; we can author applications in any NET compatible language, including Visual Basic .NET, C#, and Jscript.Net. Additionally the entire .NET Frame work is available to any ASP.NET application.

Developers can easily access the benefits of these technologies, which include the managed common language runtime environment, type safety, inheritance, and so on.

ASP.NET has been designed to work seamlessly with WYSIWYG HTML editors and other programming tools, including Microsoft Visual studio .NET. Not only does this make Web development easier, but it also provides all the benefits that these tools have to offer, including a GUI that developers can use to drop server controls onto a web page and fully integrated debugging support.

Web Forms allows us to build powerful forms-based Web pages. When building these pages, we can use ASP.NET server controls to create common UI elements, and program them for common tasks. These controls allow us to rapidly build a Web Form out of reusable built-in or custom components, simplifying the code of a page.

ASP.NET takes advantage of performance enhancements found in the .Net Framework and common language runtime. Additionally, it has been designed to offer significant performance improvements over ASP and other Web development platforms. All ASP.NET code is compiled, rather than interpreted, which allows early binding, strong typing, and just-in-time(JIT) compilation to native code, to name only a few of its benefits.ASP.NET is also easily factorable, meaning that developers can remove modules (a session module, for instance) that are not relevant to the application they are developing.

ASP.NET provides extensive caching services (both built-in services and caching APIs). ASP.NET also ships with performance counters that developers and system administrators can monitor to test new applications and gather metrics on existing applications.

Writing custom debug statements to your Web page can help immensely in troubleshooting your application's code. However, it can cause embarrassment if it is not removed. The problem is that removing the debug statements from your pages when your application is ready to be ported to production server can require significant effort.

ASP.NET offers the Trace Context class, which allows us to write custom debug statements to out pages as we develop them. They appear only when your have enabled tracing for a page or entire application. Enabling tracing also appends details about a request to the page, or, if you so specify, to a custom trace viewer that is stored in the root directory of your application.

3.3.2 SQL SERVER

MICROSOFT SQL SERVER 2000

It is a relational database management system (RDBMS) produced by Microsoft. Its primary query language is Transact-SQL, an implementation of the ANSI/ISO standard Structured Query Language (SQL) used by both Microsoft and Sybase.

Data can be defined and manipulated in a table with SQL statements. SQL's data definition language (DDL) statements are used to define data. DDL statements include statements for creating and altering databases and tables.

Update, delete, or retrieve a data in a table are done by SQL's data manipulation language (DML). DML statements include statements to alter and fetch data. The most common SQL statement is the SELECT statement, which retrieves data from the database.

In addition to SQL statements, the Oracle server has a procedural language called PL/SQL. PL/SQL enables programmers to program SQL statements. It lets user control the flow of a SQL program, use variables, and write error-handling procedures.

DATA DEFINITION LANGUAGE (DDL) STATEMENTS:

Data definition language statements define, maintain, and drop schema objects when they are no longer needed. DDL statements also include statements that permit a user to grant other users the privileges, or rights, to access the database and specific objects within the database.

DATA MANIPULATION LANGUAGE (DML) STATEMENTS:

Data manipulation language statements manipulate the database's data. For example, querying, inserting, updating, and deleting rows of a table are all DML operations. Locking a table or view and examining the execution plan of an SQL statement are also DML operations.

CHAPTER 4

SYSTEM DESIGN AND DEVELOPMENT

4.1 ELEMENTS OF DESIGN

System Design is the most creative and challenging phase in the development of a software system. Design implies to a description of the final system and the process by which it is developed. The first step is to determine what input data is needed for the system and then to design a database that will meet the requirements of the proposed system. The next step is to determine what outputs are needed from the system and the format of the output to be produced.

During the design of the proposed system some areas where attention is required are:

- What are the inputs required and the outputs produced?
- How should the data be organized?
- What will be the processes involved in the system?
- How should the screen look?

The steps carried out in the design phase are as follows:

- Modular Design
- Input Design
- Output Design
- Database Design

4.1.1 MODULAR DESIGN

It is always difficult for any System Development team to grasp a system without breaking it into several subsystems/modules. These subsystems/modules will be a part of

the original system yet they will be independent in the sense that they will incorporate within them the major functionalities of the proposed system.

A software system is always divided into several subsystems/modules which make it easier to develop and perform tests on the whole system. The subsystems are also known as the modules and the process of dividing an entire system into subsystems/modules is known as Decomposition.

The modules identified for the proposed Dual Security enhancement Process are as below:

- Web portals security
- Sha1 encryption algorithm
- Streaming data security
- Static data security

WEB PORTAL SECURITY

Portal Security is based on the CAPTCHA security RunTime and protects – web portals - also SOA infrastructures.

- To comprehensively protect company portals.
- To realize Single-Sign-On from Portal to Backend system.
- To protect portals and web applications against viruses and malware.
- To repel Web attacks safely and efficiently
- To implement flexible Security functionality and filter

SHA1 ENCRYPTION ALGORITHM

The SHA1 encryption algorithm specifies a Secure Hash Algorithm (SHA1), which can be used to generate a condensed representation of a message called a message digest. The SHA1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required. Both the transmitter and intended receiver of a message in computing and verifying a digital signature uses the SHA1.

SHA1 is used for computing a condensed representation of a message or a data file. When a message of any length < 2 64 bits is input, the SHA1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

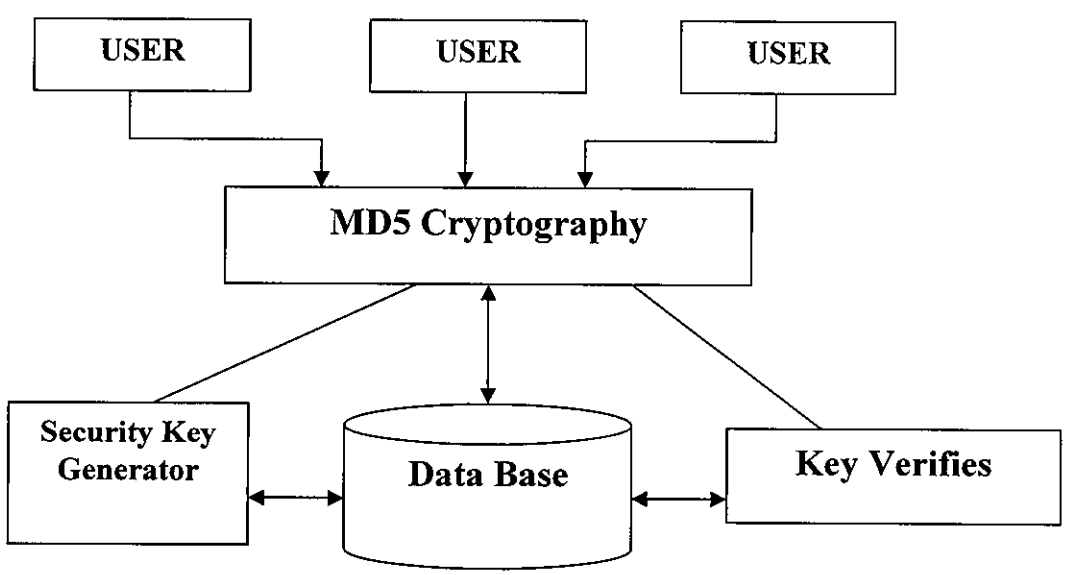
The SHA1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA1 is a technical revision of SHA (FIPS 180). A circular left shift operation has been added to the SHA (FIPS 180). SHA1 improves the security provided by the SHA standard. The SHA1 is based on principles similar to those used by the MD4 message digest algorithm.

STREAMING DATA SECURITY

Once SHA1 algorithm is generated by using that we can control the streaming data. Streaming data denotes that transfer of information from server to client and vice versa

STATIC DATA SECURITY

Static data denoted that important document present in the particular web portal or in standalone machine. Here we are using strong cryptography algorithm to protect the data from hackers



4.1.2 INPUT DESIGN

The designs Decisions for handling input specify how data are accepted for computer processing. The design specifies the means by which the end user and the system operators direct the system in which action to take. Online system include a

Dialogue or conversation between the user and the system. The input design is the link that ties the information system in to the world of its users.

Objective Input Design

Input Design consists of developing specifications and procedures for data preparations and data entry. The following objectives are to be achieved.

Controlling the amount of Input

Data preparation and data entry depends on people. The costs get high if the input is high. The input phase of computing is slow which leaves the system idle consuming more time. The major reason for controlling the amount of input are, first, as the lab our is high; the cost of preparing the data and entering the data is also high. Second, the input phase of computing can be a slow process that can take many times longer than the time needed by computers to carry out their tasks. By reducing input requirements, thes analyst can speed the entire process from data capture to processing to providing results to users

Avoiding Delay

The delay in data entry and data preparation is called Bottleneck. Avoiding this bottleneck should be the objective of the analyst designing the input. in one sense, the rate at which errors occur depends on the quantity of data, since the smaller the amount of data input ,the fewer the opportunities for errors. The manner in which the data is entered also affects the occurrence of error .Another aspect of avoiding errors is the need to detect the error when they do occur. These are done using input validation techniques.

Avoiding Errors in Data

Reducing the volume of data can reduce the number of errors. Validation techniques can be used to avoid errors while Data entry it self.

Avoiding Extras Steps

Sometimes volume of data gets uncontrollable. To be effective avoid input design with extra steps. When the volume of transaction can't be reduced, the analyst must be sure the process is as efficient is possible. The analyst must also avoid input design that causes extra steps.

4.1.3 OUTPUT DESIGN

Output refers to the results information that is generated by the system. Designing the computer output should proceed in a well organized, well thought out manner. The right output must be developed while ensuring that each output element is designed so that people will find system easy to use effectively. The basis of the output generated is to evaluate the usefulness of the application.

The arrangement of information on a display, or a printed document is termed as a layout. The output design is specified on layout forms, sheets that describe the location characteristics and the format of the column headings and pagination. Output design phase of system is concerned with the convergences of information to the end user in user friendly manner.

The output design should be efficient, intelligible so that relationship with the end user is improved considerably and thereby, enhancing the decision-making process. The contents of the output are then defined in a detailed manner during the physical design of outputs .Certain data are in a desirable manner.

Objectives of Effective Output Design

- Convey data about the past activities, current status, projections of the future.
- Signal important events, problems, opportunities or warning.

- Trigger an action.
- Confirm an action.
- Determine what information to present.
- Decide whether to display, print, or voice the information and select the medium of output.
- Arrange the presentation of information in an acceptable format.
- Decide how to distribute the output to intended recipients.

4.1.4 DATABASE DESIGN

A database is a collection of inter-related data stored with minimum redundancy to serve many users quickly and efficiently. The general objective of database design is to make the data access easy, inexpensive and flexible to the user. An elegantly designed database can play a strong foundation for the whole system.

The database is used to group data into a number of tables and minimize the artificiality embedded in using separate files.

The details about the relevant data for the system are first identified. According to their relationship, tables are designed through the following method.

NORMALIZATION

- Refinement process is called Normalization
- Refinement process eliminates the Inconsistency, Uncertainty and Redundancy in the database.
- Defined as a step-by-step process of decomposing a complex relation into a simple and stable data structure.
- The formal process that can be followed to achieve a good database design.
- The different stages of normalization are known as "normal forms".
- All tables in Dual Security enhancement Process are carried out by using first normal form, second normal form and third normal form.

4.2 TABLE STRUCTURE

DESIGN CONVENTIONS USED

1. Appropriate words that describe the table should be used.
2. No special character is used in formulating a table name.
3. No number should be used anywhere in the table name string.

TABLES

The following tables have been created for Dual Security Enhancement Process

Table Name : Login Details

S.No	Field Name	Data type	Description
1	UserId	Int	Unique id for user
2	Password	nvarchar(10)	Minimum six characters

TABLE 4.2.1 LOGIN DETAILS

Table Name : AccountInformation

Primary key : Acc Id

S.No	Field Name	Data type	Description
1	Accid	Int	Unique id for account
2	PrfileID	nvarchar(50)	Enter the name of the user
3	Email	nvarchar(50)	Enter the email id
4	Password	nvarchar(10)	Password
5	Gender	Int	Specify male or female
6	DOB	nvarchar(50)	Date of birth
7	ReligonComm	nvarchar(50)	Specify the caste
8	Country	nvarchar(50)	Enter country
9	Status	Bit	Check the status
10	Creby	Int	Created by
11	CreDate	Datetime	Date of creation

TABLE 4.2.2 ACCOUNT INFORMATION

Table Name : Captcha secure

Primary Key : Cap id

S.No	Field Name	Data type	Description
1	CaptchaID	Int	Unique id for captcha
2	Capques	nvarchar(500)	Enter the question for captcha
3	Capans	nvarchar(250)	Answer the suitable question
4	Credate	Date/time	Date creation
5	Moddate	Date/time	Modify the date
6	CreBy	nvarchar(50)	Created By
7	ModBy	nvarchar(50)	Modify By

TABLE 4.2.3 CAPTCHA SECURE

Table Name : Encrypt

Primary Key : Encrypt id

Foreign Key : User id

S.No	Field Name	Data type	Description
1	Encryptid	Int	Enter id for encryption
2	Userid	Int	Enter user id
3	Video	image	Upload the video
4	Vname	nvarchar(50)	Enter the name
5	Videoname	nvarchar(50)	Name of the video
6	Videosize	Bigint	Size of the video

TABLE 4.2.4 ENCRYPT

Table Name : Photo

Primary Key : photoid

Foreign Key : Accnt id

S.No	Field Name	Data type	Description
1	Photoid	Int	Create photo id
2	Accntid	Int	Enter account id
3	Filename	nvarchar(150)	Display the filename
4	Fileext	nvarchar(50)	Extension of the file
5	Photoimg	Image	Upload the image
6	Filesize	Int	Size of the file
7	Contype	nvarchar(40)	Content type
8	Creby	nvarchar(30)	Created by

TABLE 4.2.5 PHOTO

Table Name : Profile Information

Primary Key : Profiledetail id

Foreign Key : Accnt id

S.No	Field Name	Data type	Description
1	Profiledeailid	Int	Enter profile details id
2	Accntid	Int	Account id
3	Profilecreby	Int	Profile created by whom
4	Name	nvarchar(40)	Enter the name
5	Gender	int	Click the gender
6	Age	Int	Type the age
7	Email	nvarchar(50)	Create email for user
8	Maritalstatus	Int	Status of the marriage
9	Havechild	Int	Click children are available or not
10	Bodytype	Int	Type of body
11	Complexion	Int	Select weather it is fair or medium
12	Height	Int	Select their height
13	Mothertongue	nvarchar(50)	Select the mother tongue
14	Caste	nvarchar(50)	Select their caste
15	Dosham	Int	Click the dosham
16	State	nvarchar(20)	Enter the state
17	City	nvarchar(20)	Enter the city
18	Education	nvarchar(50)	Qualification for education
19	Profession	nvarchar(40)	Select their professions
20	Familyvalue	Int	Click the family value
21	Diet	Int	Select the diet
22	Smoke	Int	Smoking
23	Drink	Int	Drinking
24	Specialcase	nvarchar(30)	Any special case
25	Aboutself	nvarchar(3000)	Type their details
26	Country	nvarchar(50)	Enter the country
27	TelephoneType	Int	Type of telephone number

28	TelephoneNo	Int	Telephone number
29	VisibleTo	Int	Visible to
30	CreBy	nvarchar(40)	Created by
31	CreDate	Datetime	Date of creation
32	Flag	Bit	Flag

TABLE 4.2.6 PROFILE INFORMATION

Table Name : Secure Data

Primary Key : Secid

S.No	Field Name	Data type	Description
1	Secid	Int	Create id for security
2	Name	nvarchar(40)	Enter the name
3	Emailid	nvarchar(50)	Enter the email
4	Message	nvarchar(500)	Type the message
5	Encrypmsg	nvarchar(500)	Encrypt the message
6	Credate	Datetime	Date creation
7	Moddate	Datetime	Modify date

TABLE 4.2.7 SECURE DATA

Table Name : Users

Primary key : Accnt id

S.No	Field Name	Data type	Description
1	Accntid	Int	User create an id
2	Name	nvarchar(50)	Enter the name
3	UserId	nvarchar(50)	Create user id
4	Password	nvarchar(50)	Password
5	Address	nvarchar(200)	Enter the address
6	EmailID	nvarchar(50)	Create email id
7	Pincode	nvarchar(10)	Enter the pincode
8	PhoneNo	Int	Enter the phone number
9	Status	Bit	Check the status

TABLE 4.2.8 USERS

Table Name : Video

Primary Key : Video id

Foreign Key : User id

S.No	Field Name	Data type	Description
1	Videoid	Int	Create video id
2	Userid	Int	Enter user id
3	Video	Image	Upload video
4	Videoname	nvarchar(50)	Name of the video
5	Videosize	Bigint	Size of the video

TABLE 4.2.9 VIDEO

4.3 USECASE DIAGRAM

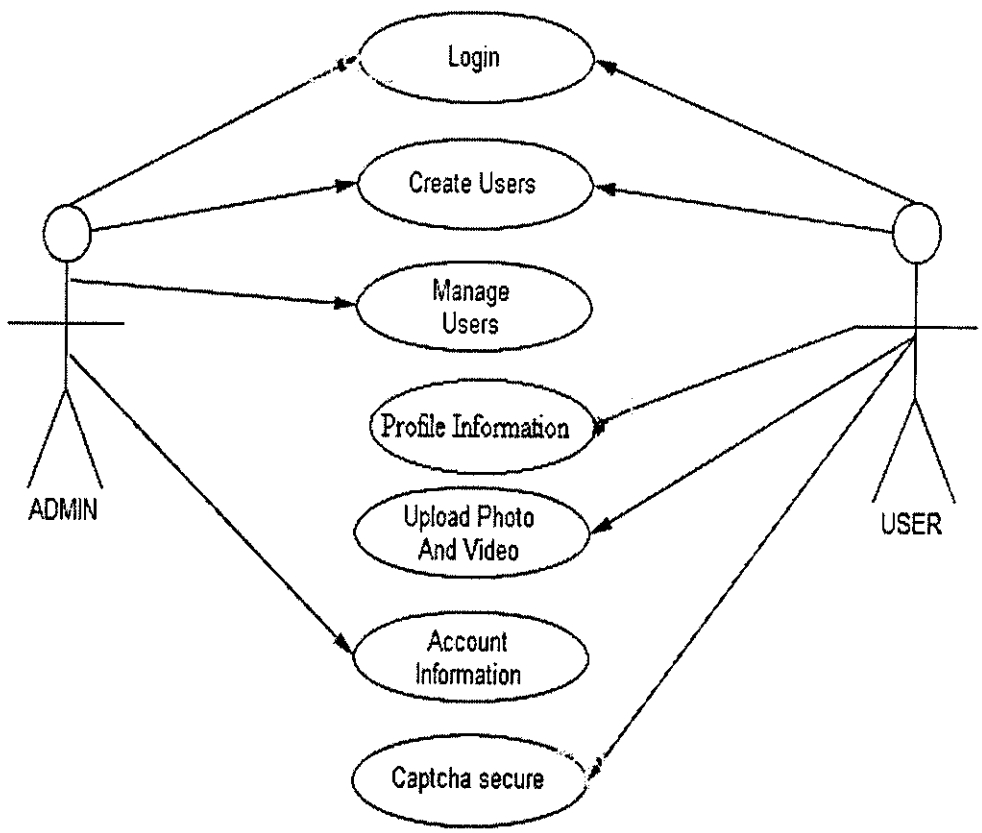


Figure 4.3.1 Use case Diagram for Admin Vs User

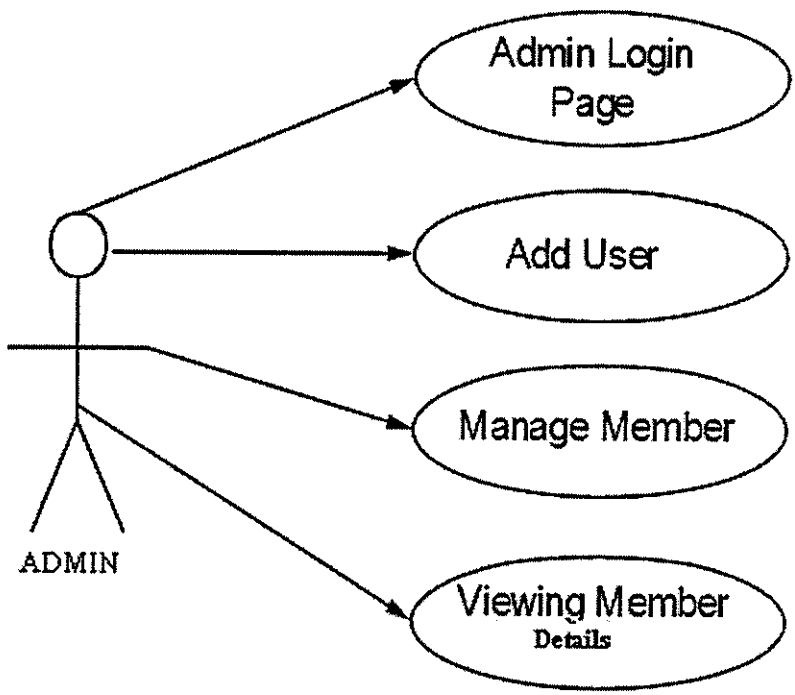


Figure 4.3.2 Use case Diagram for Admin

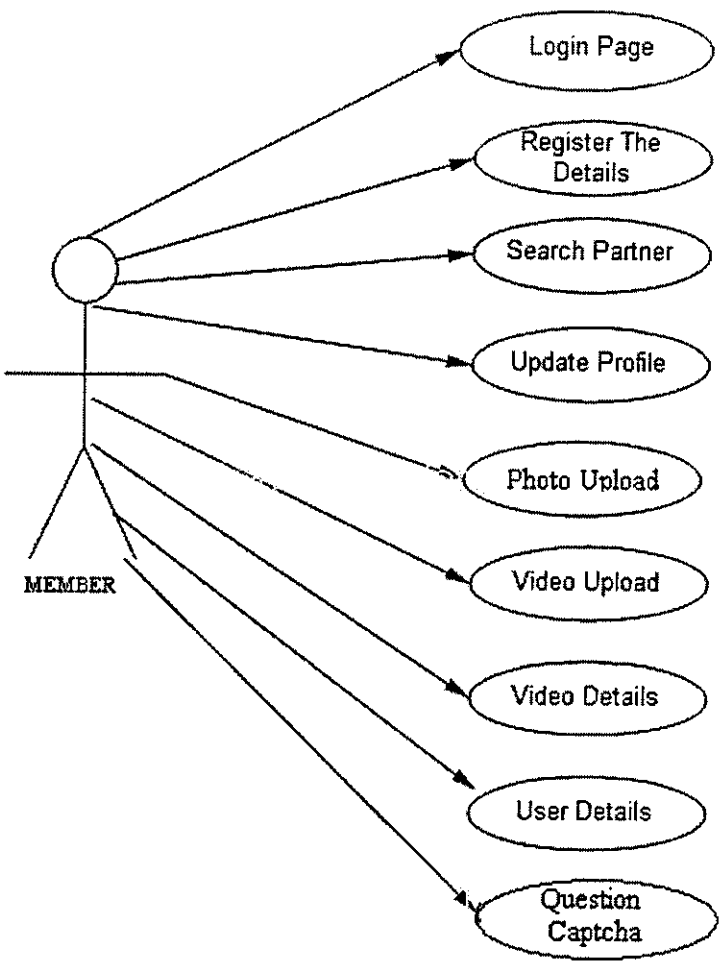
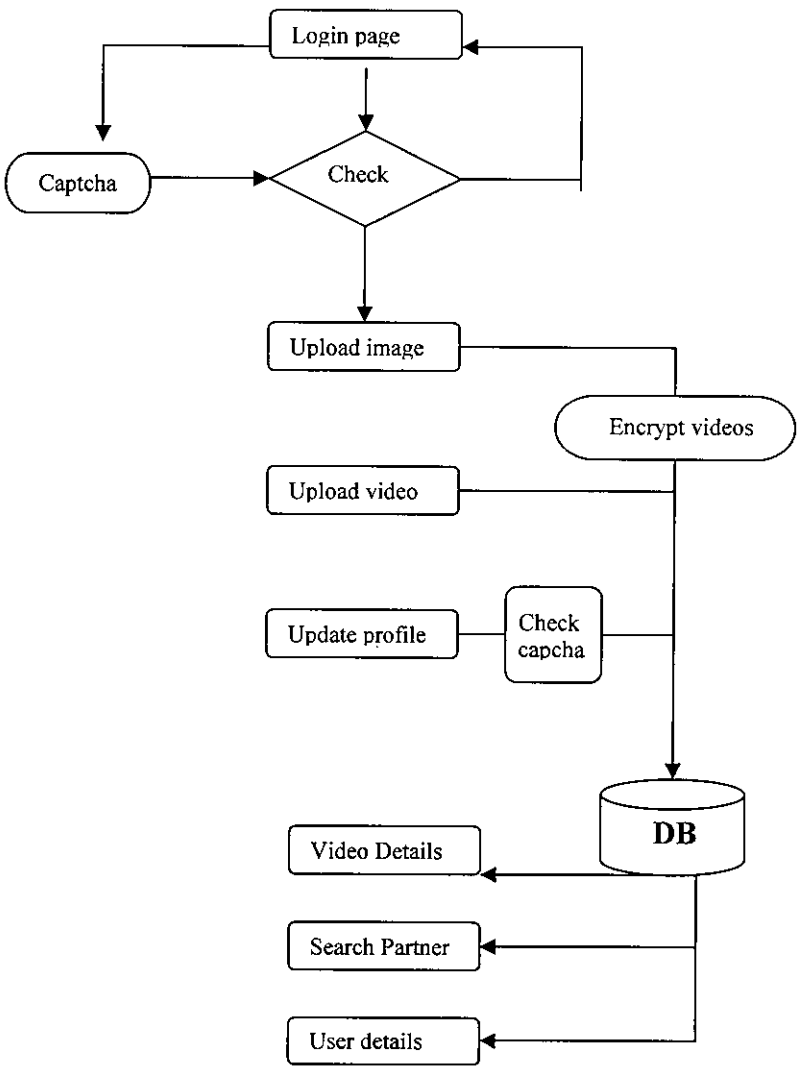


Figure 4.3.3 Usecase Diagram for Member

4.4 Over All System Architecture



CHAPTER 5

SYSTEM TESTING AND IMPLEMENTATION

System Testing and Implementation is the part of the software engineering life cycle, where, the design artifacts are converted to a working application. Coding is done in this stage using an apt framework and programming language, which would solve the specific problem the best way. Once the design is coded into a working application, it has to be verified, validated and tested in detail. The tested product if successful is deployed in the user environment.

5.1 SYSTEM VALIDATION

Validation testing is one, which checks the given data is a valid one, or not. In our system, first stage username and password is checked. If it is a valid one, then the services will provided to the user. Hence validation testing takes place at the earlier part of our project. This is one of the most crucial one, which takes place at the all kind of projects.

5.2 TESTING

Testing is a critical element of software quality and assurance and represents the ultimate review of specification design and coding. It is a vital activity that has to be enforced in the development of any system. This could be done in parallel during all the phases of system development. The feedback received from these tests can be used for further enhancement of the system under consideration. The testing phase conducts test using the Software Requirement Specification as a reference and with the goal to see whether the system satisfies the specified requirements.

The main types of tests carried out on Dual Security Enhancement Process are:

- Unit Test
- Integration Test
- System Test

5.2.1 UNIT TESTING

Module or Unit Testing is the process of testing all the program units that make up a system. Unit testing focuses on an individual module thus allowing one to uncover all the errors made logically and while coding in the module.

In Dual security Enhancement Process each page is tested separately as a unit. Initially the flow of control and data through that page is checked. When considering a module as a unit, the flow of data and control through the whole module is tested. The result is stored in the test plan. In a page, each control is further tested in unit testing. The process is done in all the pages of the system. Once the errors are rectified, the testing procedure is repeated with same test cases to ensure this hasn't produced new errors. Hence this is a continuous process.

5.2.2 INTEGRATION TESTING

Integration testing tests the process of integrating the various modules to form the completed system. Integration starts with a set of units each individually tested in isolation and ends when the entire application has been built. Integration testing verifies that the combined units function together correctly. It facilitates in finding problem that occur at interface or communication between the individual parts.

Dual Security Enhancement Process followed top-down integration testing. Modules were linked to the main menu in a sequence as required in the real time operating mode of the system. Menu items were created as and when required for the integration. This process is continued from the page level to module level, finally to the system level. In the final stage, the whole system is taken together and tested for integration. A change in one place should be reflected through out the system. Regression testing is done after each change made into the software. This tests if the change has affected any part of Dual Security Enhancement Process negatively after the change was made. The whole set of test cases need to be run again to do the regression testing.

5.2.3 SYSTEM TESTING

System testing is actually a serious of different tests, whose primary purpose is to fully exercise the computer-based system. This helps in verifying that all the system elements have been properly integrated and perform the allocated functions. It verifies the entire product after having integrated all software and hardware components, and validates it according to the original project requirement. The system testing takes into consideration the hardware, and the software.

5.2.3.1 SECURITY TESTING

Security testing is important in system testing. The system in no way shall be accessible to unauthorized users. Testing is done to ensure that a user with respective rights can only view the various forms and reports presented by Dual Security Enhancement Process. If users try to perform something beyond his assigned rights corresponding messages should be displayed. The Dual Security Enhancement Process in such cases displays an error message.

Another security issue involves the sensitive data in the system. The system is highly secure with authentication fixed at various levels of the hierarchy.

One more level of security is concerned with user rights. Each user is applied rights module wise. The menus can be configured to roles. Users can also be configured to roles. Menu items are assigned to users dynamically based on the roles assigned to menu items as well as users. A match is done before displaying the menu to the user. Different Menu items are displayed for user and administrator.

5.2.4 TEST CASE

		Test Case for Dual Security	
Login Page			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Log01	Enter the wrong pass and userid	Enter password and userid	It display the Invalid user name and password
Log02	Enter the correct pass and userid	Enter password and userid	It goes to user home page
Log3	before admin approve the account	Enter password and userid	you are not approve by admin
Log4	to check whether captcha is displayornot in login page	Enter 4 times wrong userid and pwd	It display the question captcha
Update Profile			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Up01	Fill the field with incorrect values	Wrong Email Entry	it displays Check Email
Up02	checking the Name giving with number	Enter number	it displays Check name
Up03	whether update profile is update button is working or not	Submit the values	it display error values
Registration			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Reg1	to check email validation	Enter incorrect email id	it display check email
reg2	to check email comparison	Enter two different email in two field	To check Email is not equal
reg3	to check pwd	leave to enter pwd	Enter pwd

reg4	to check pwd comparison	To enter two different pwd	Check com pwd
Reg5	whether acception correct email	Enter correct email	No msg
reg6	to checking captcha	Enter Wrong no	check image no is not equal
Reg7	to submit the button without filling anyvalues	submit the button	it display check email,pwd,image no
Reg8	to give all fields are correct values	Enter the appropriate value	Your Account created Successfully!!
Reg9	to pwd is encrypted or not	Enter values	Ok
Upload Image			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Img01	To check image is uploading or not	Import the image	Ok
Img02	to display image	Imort	Displaying
Video Upload			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Vid01	To check image is uploading or not	Import the video	Ok
Vid01	to check playing the video	import the video	Playing
Logout			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Log01	to check the logout is working or not	click logout button	Login page to display
Log02	To check session expired	wait few minutes	Logout the current page
Admin Page			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
Log01	Enter the wrong pass and userid	Enter password and userid	It display the Invalid user name and password
Log02	Enter the correct pass and userid	Enter password and userid	It goes to user home page

Log3	before admin approve the account	Enter password and userid	you are not approve by admin
Log4	to check whether captcha is displayornot in login page	Enter 4 times wrong userid and pwd	It display the question captcha
UserView			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
UV01	to check edit button	click edit link	goes to update page
UV02	to check values are there		Values
UV03	updating the new values	Enter values	Upate Succesfully
Add Ques Capcha			
Test ID	**Test Description**	**Test i/p**	**Expected Result**
AC01	to add question and answer	Enter ques and result	submit successfully

5.2.5 SYSTEM IMPLEMENTATION

Implementation is the state in the project where the theoretical design is turned into a working system. The most crucial stage in achieving a new successful system and giving confidence on the new system for the users that will work efficiently and effectively. The system is implemented only after thorough testing is done and if it is found to work according to the specification.

It involves careful planning, investigation of the current system and is constraints on implementation, design of methods to achieve changeover, and evaluation of the changeover methods apart from planning. Two major tasks for preparing the implementation are educating, training the users and testing the system.

Implementation Plan Preparation

The implementation process begins with the preparation of plan for implementation. According to this plan other activities are carried out. In this plan discussion has been made regarding the equipment, resources and how to test the activities. Thus a clear planner prepared for the activities.

Equipment Acquisition

According to the above plan the necessary equipment have to be acquired to implement the new system, which would include all the requirements for installing and maintaining .Net framework, Asp.net, C#, Mobile Internet Toolkit, WAP-enabled device etc.

Program Code Preparation

One of the most important development activities is coding or programming. The system flowcharts and other charts are converted into modular programs. They have to be compiled, tested and debugged.

User Training and Documentation

Once the planning has been completed the major effort in the computer department is that the user department must consist of educated and trained staff as the system becomes more complex. The success of the system depends upon how they are operated and used the system.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

The Dual security Enhancement Process enables the project team to get rid of a very tedious and time consuming process which has been followed so far. The System has been developed with good user-friendly methodologies and techniques. It provides a great degree of flexibility and has been designed in such a way so as to be able to handle future enhancements and modification when necessary. It is possible for any user to exploit the features of the system to get the maximum benefit. All the programs have been tested with sample data and live data and found to execute correctly.

Thus, the project was developed with the advanced security system to enhance the security feature of the website. We've implemented our security system in the Matrimony site which is a highly secured website now. As per the project planning, we've developed the complete site with the SHA1 security system and CAPTCHA based security system.

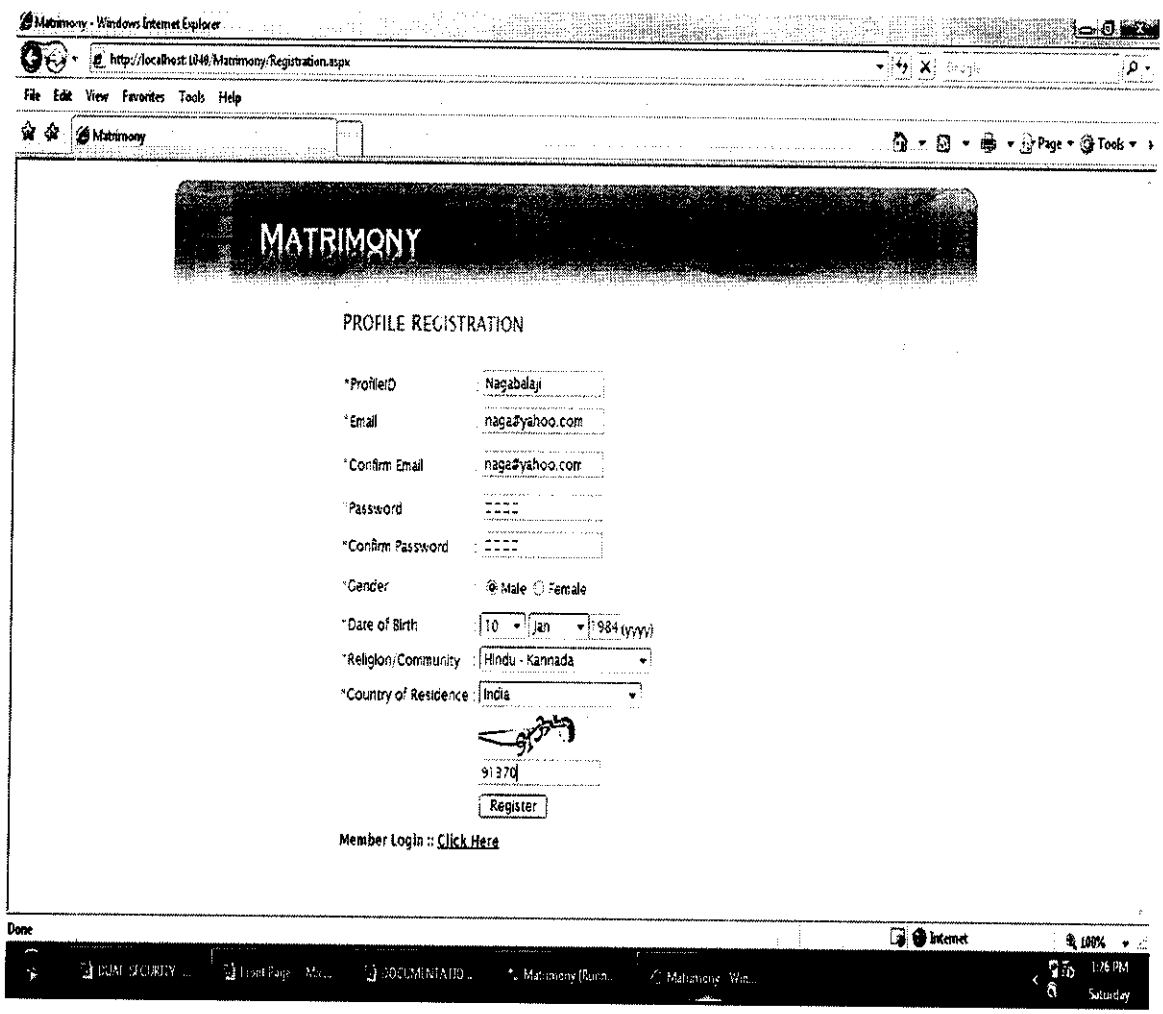
6.2 FUTURE ENHANCEMENT

The security system can be further updated as more secured system using complex and qualified developing algorithms. Currently SHA1 algorithm which is the best among all SHA algorithm series was implemented. In future, we can implement the SHA3 algorithm which is under development, which is expected to be the best over SHA1. And we can also implements the other intrusion detection system (IDS) which will be client based IDS to prevent from the intruder. This will add up more security to our current system.

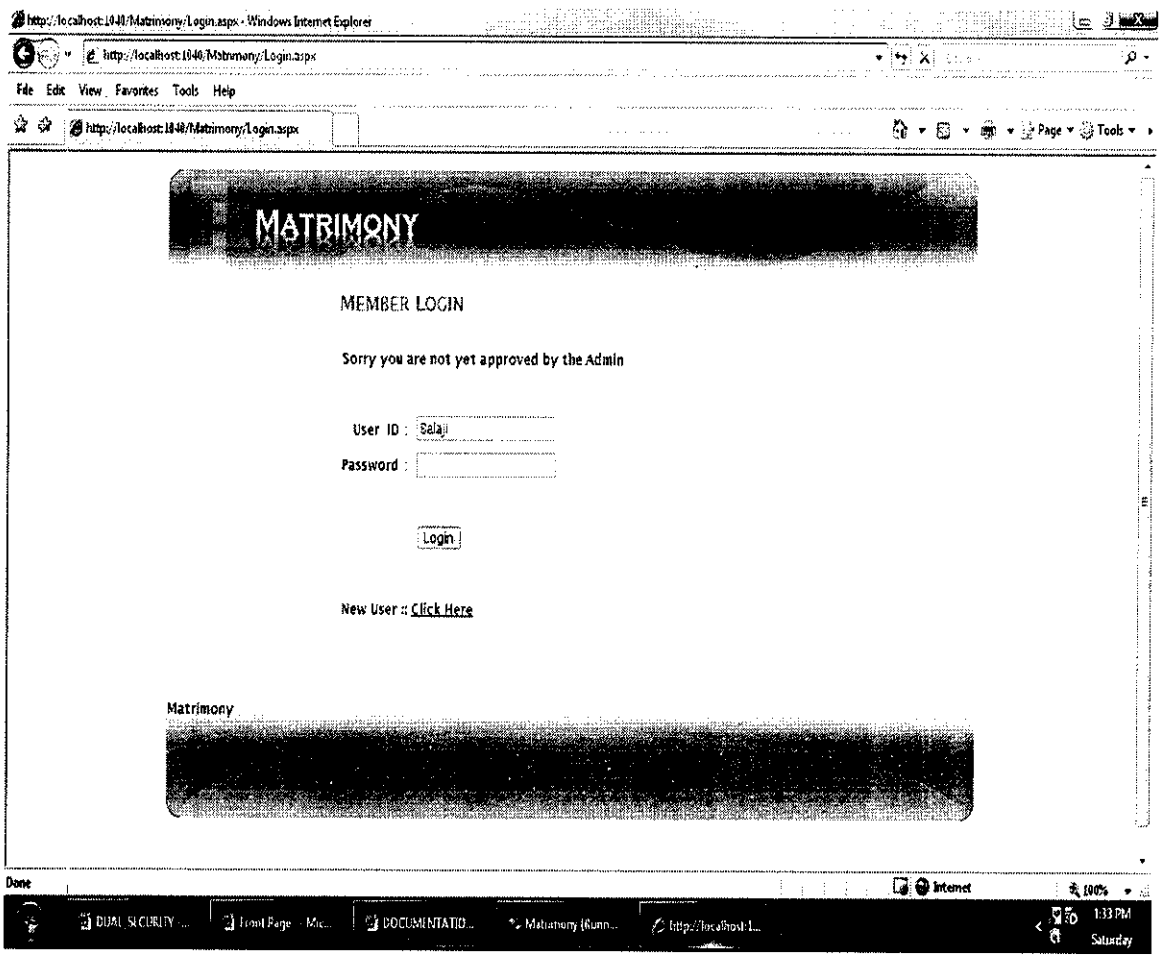
7. APPENDIX

7.1 SCREEN SHOTS

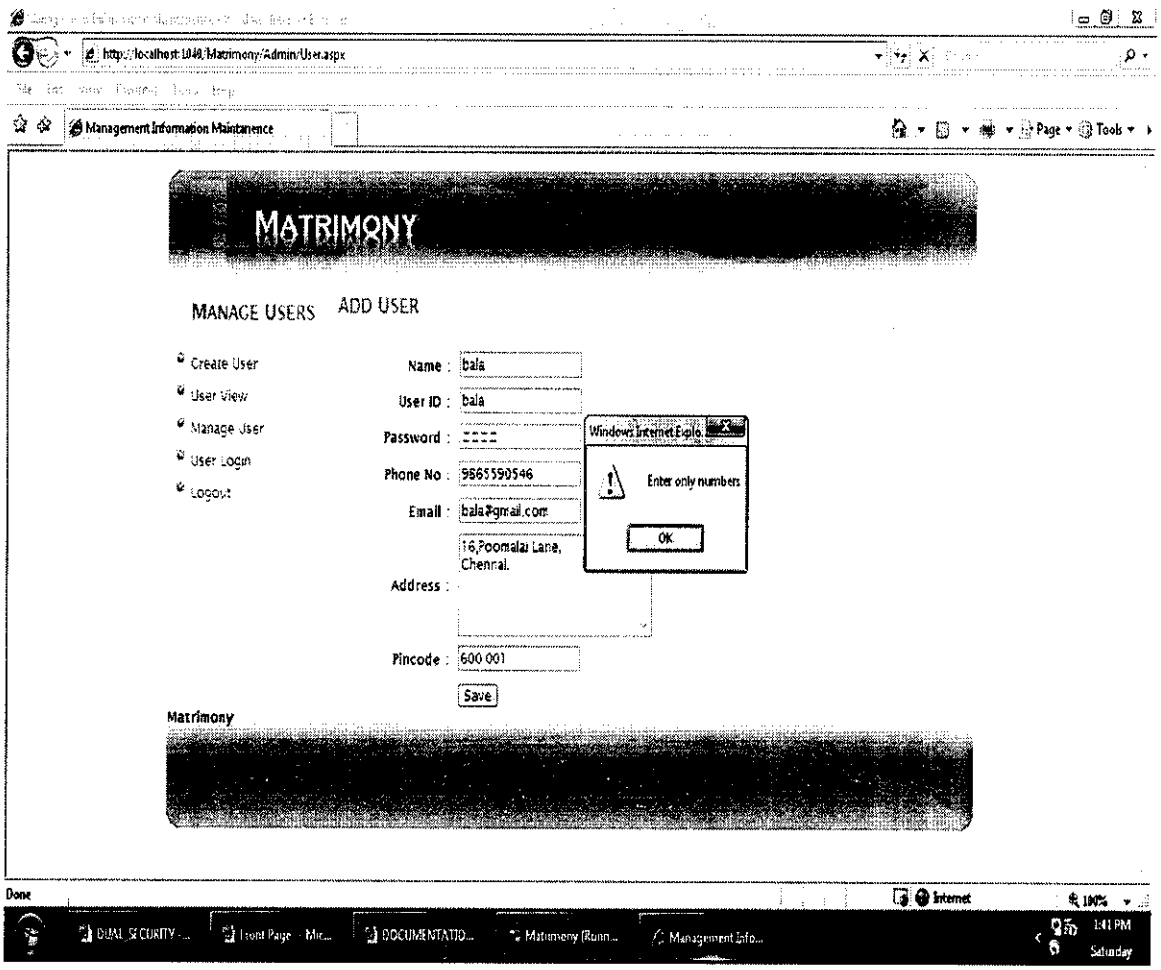
PROFILE REGISTRATION



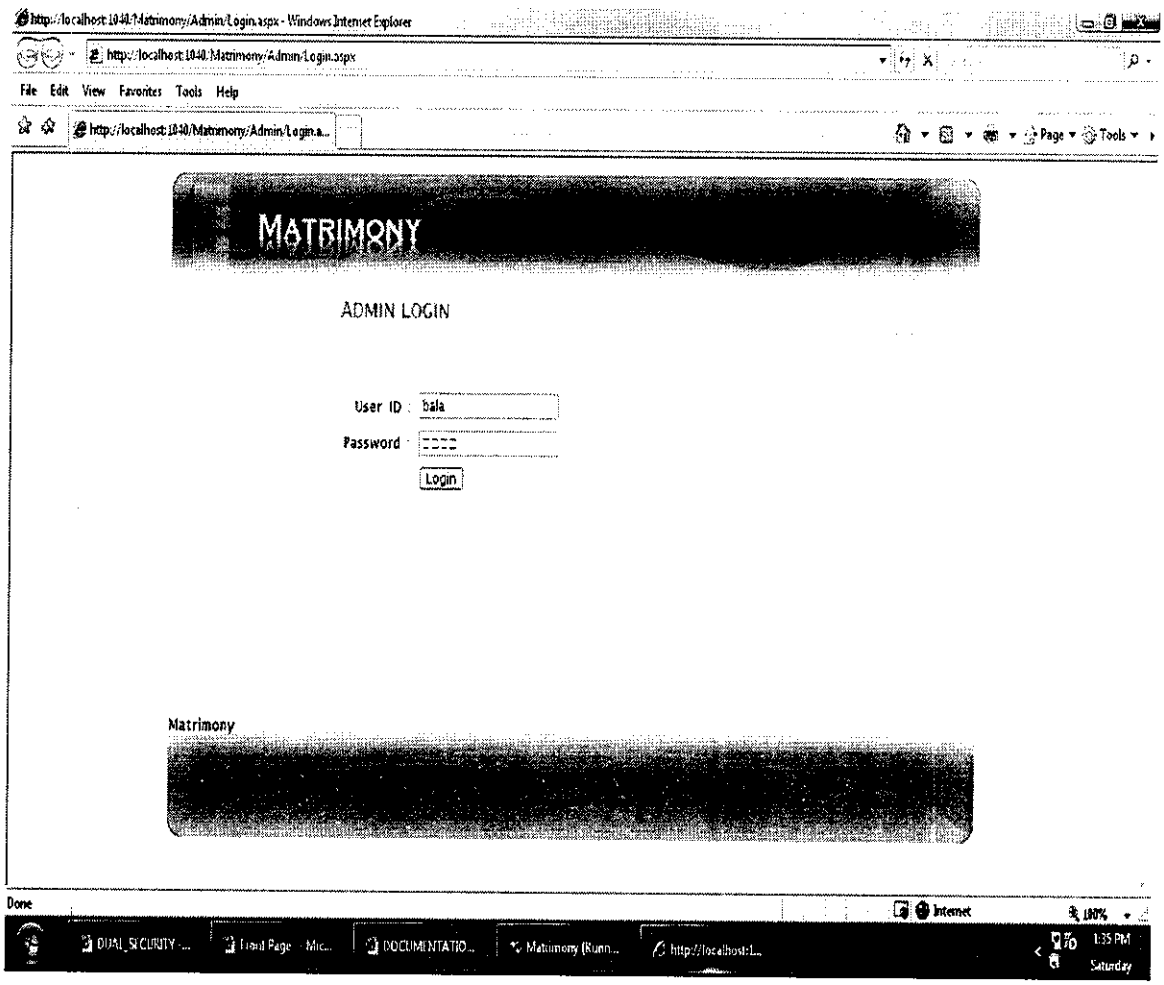
ADMIN NOT APPROVED



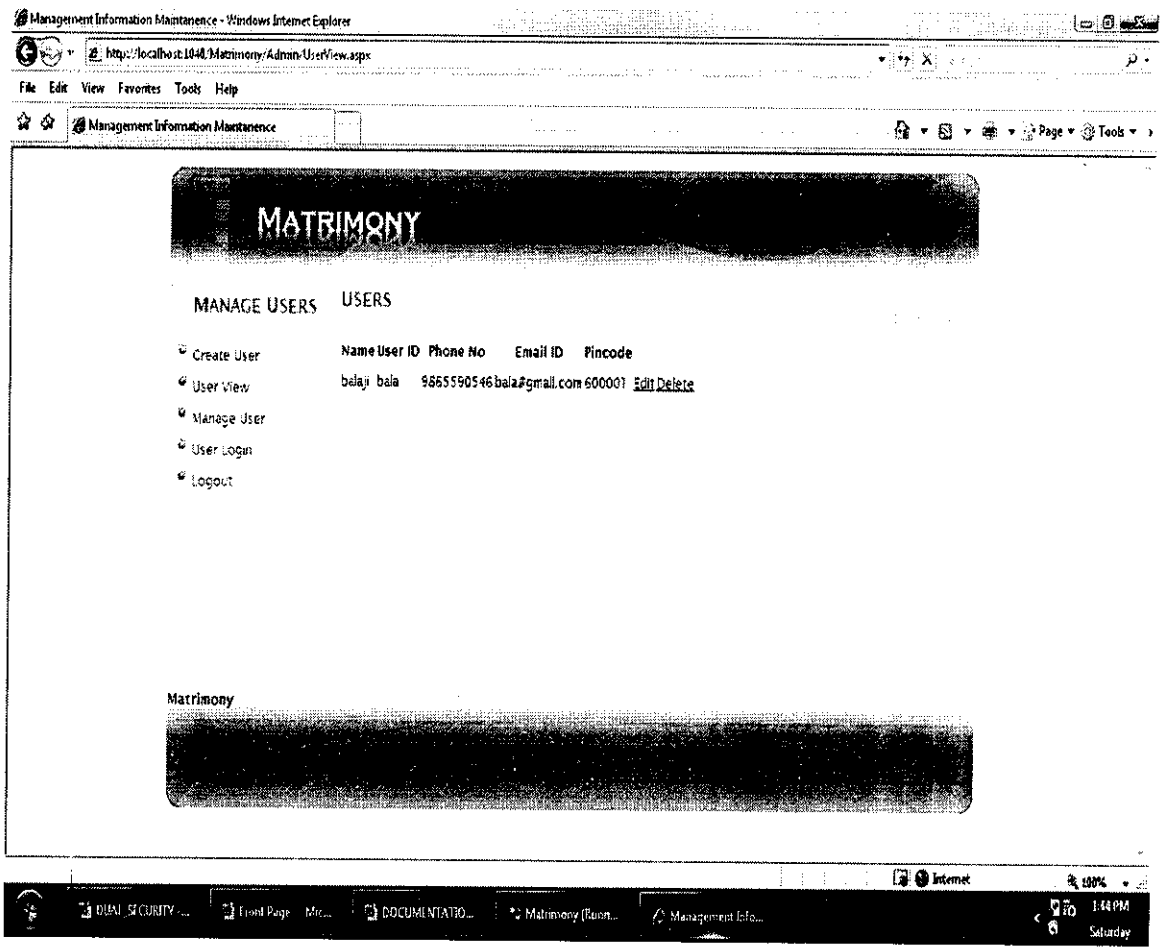
CREATE ADMIN



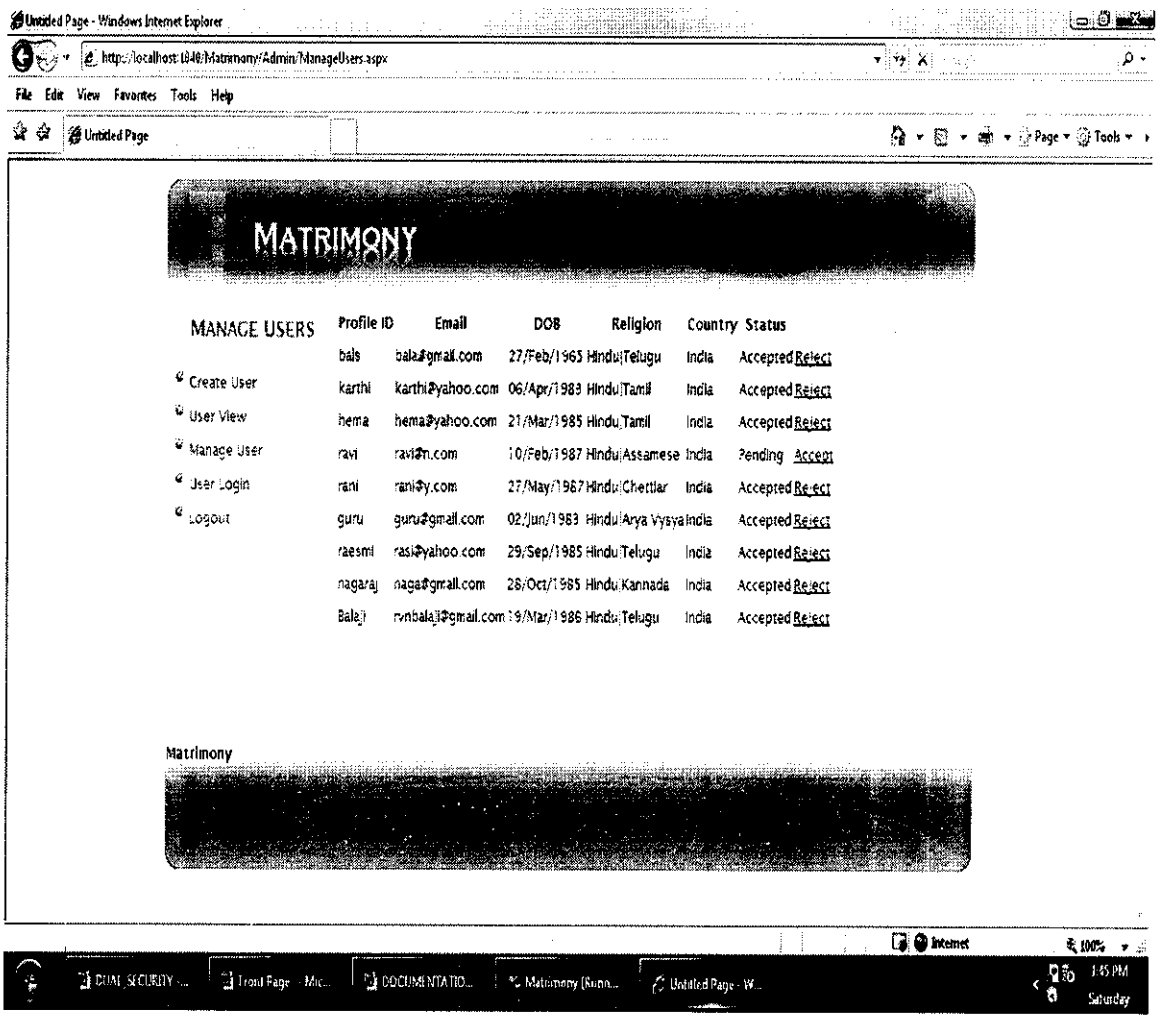
ADMIN LOGIN


MATRIMONY
ADMIN LOGIN
User ID
bala
Password
Login
Matrimony

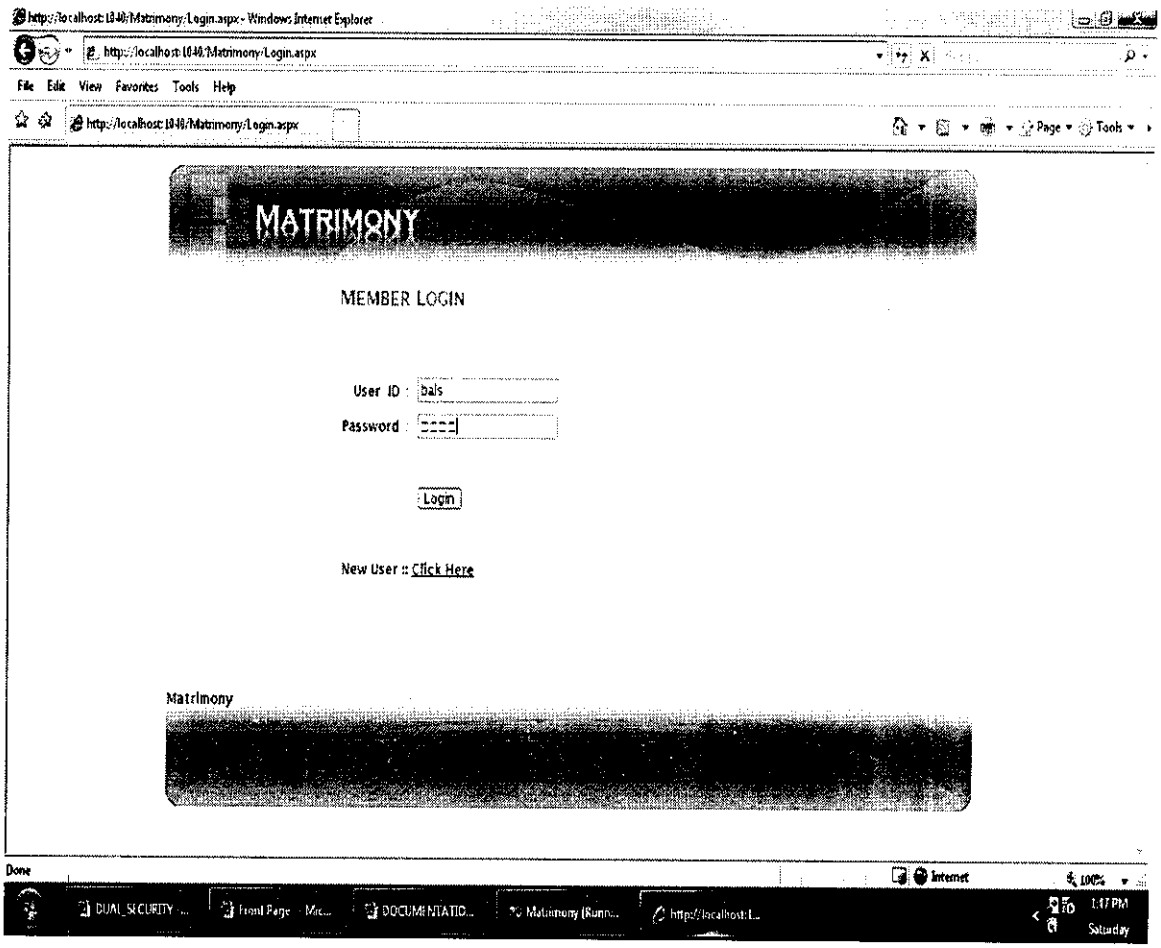
USER VIEW


Management Information Maintanence - Windows Internet Explorer
http://localhost:1048/Matrimony/Admin/UserView.aspx
File Edit View Favorites Tools Help
Management Information Maintanence
MATRIMONY
MANAGE USERS
USERS
Create User
User View
Manage User
User Login
Logout
Name User ID Phone No Email ID Pincode
balaji bala 9865590546 bala@gmail.com 600001 Edit Delete
Matrimony
Internet
100%
1:44 PM
Saturday

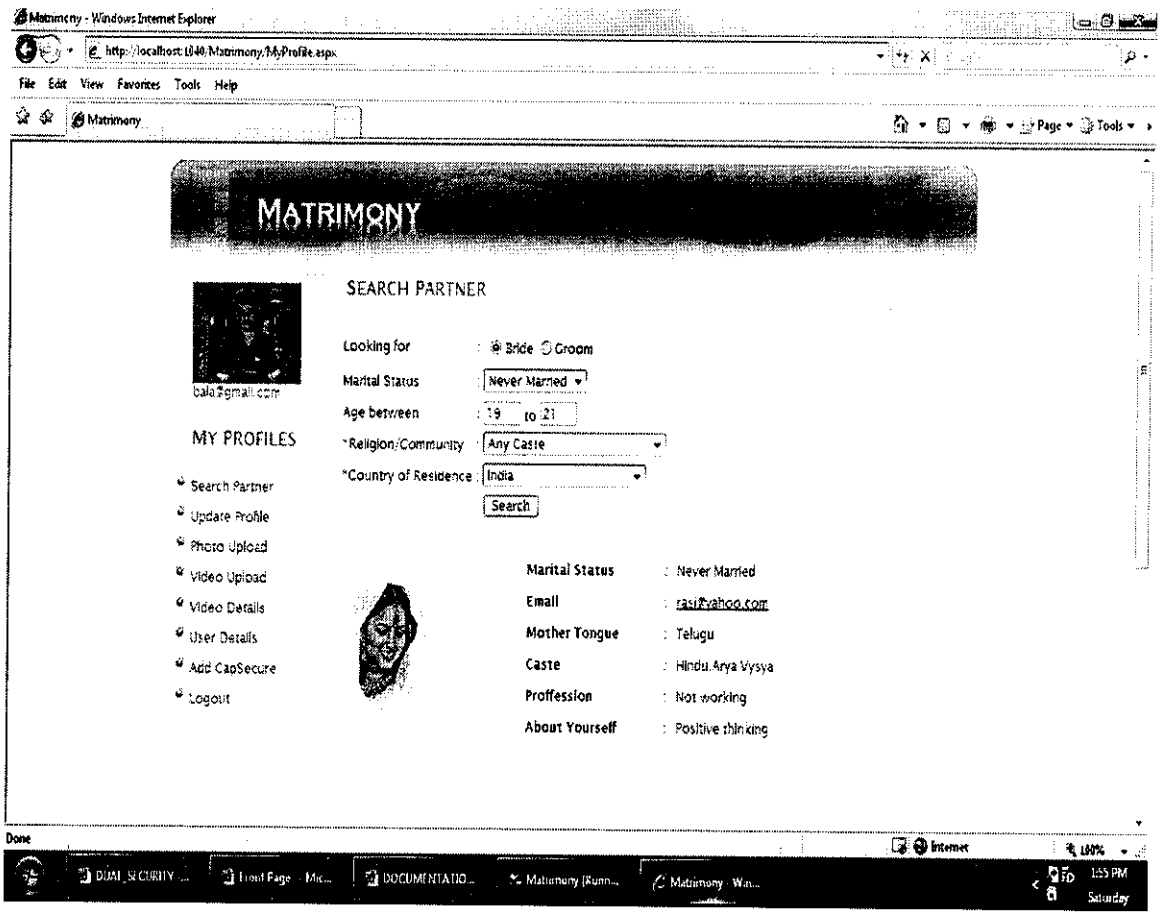
MANAGE USER


Untitled Page - Windows Internet Explorer
http://localhost:1040/Matrimony/Admin/ManageUsers.aspx
File Edit View Favorites Tools Help
Untitled Page
MATRIMONY
MANAGE USERS
Create User
User View
Manage User
User Login
Logout
Profile ID Email DOB Religion Country Status
bala bala@gmail.com 27/Feb/1965 Hindu|Telugu India Accepted Reject
karthi karthi@yahoo.com 06/Apr/1983 Hindu|Tamil India Accepted Reject
hema hema@yahoo.com 21/Mar/1985 Hindu|Tamil India Accepted Reject
ravi ravi@m.com 10/Feb/1987 Hindu|Assamese India Pending Accept
rani rani@y.com 27/May/1967 Hindu|Chettiar India Accepted Reject
guru guru@gmail.com 02/Jun/1983 Hindu|Arya Vysya India Accepted Reject
raesmi rasi@yahoo.com 29/Sep/1985 Hindu|Telugu India Accepted Reject
nagaraj naga@gmail.com 28/Oct/1985 Hindu|Kannada India Accepted Reject
Balaji rvnbalaji@gmail.com 19/Mar/1986 Hindu|Telugu India Accepted Reject
Matrimony
Internet
100%
1:45 PM
Saturday

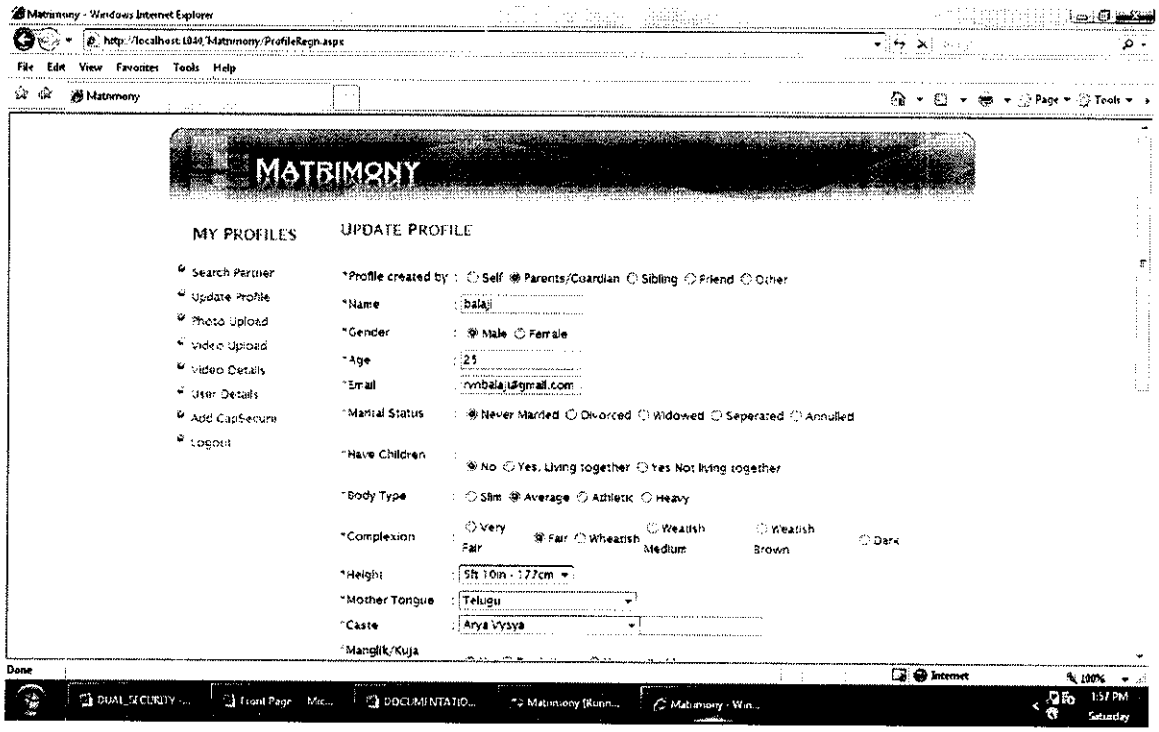
USER LOGIN


MATRIMONY
MEMBER LOGIN
User ID : bals
Password :
Login
New User :: Click Here
Matrimony

SEARCH PARTNER



UPDATE PROFILE



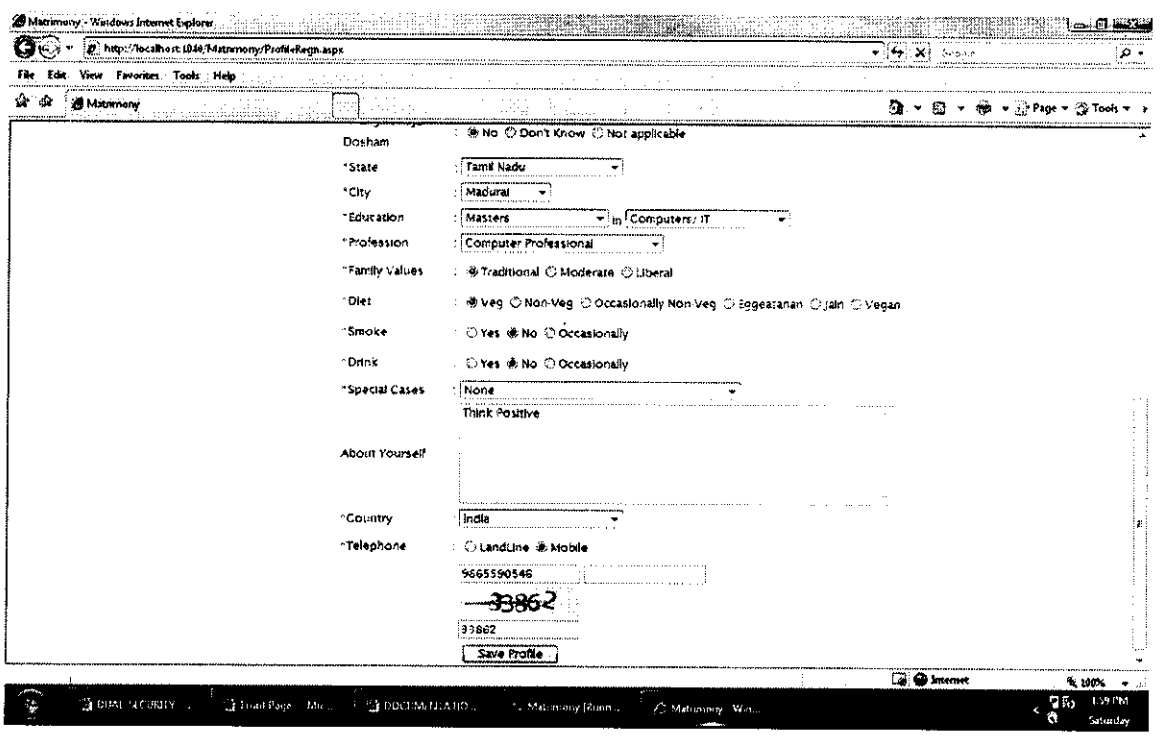
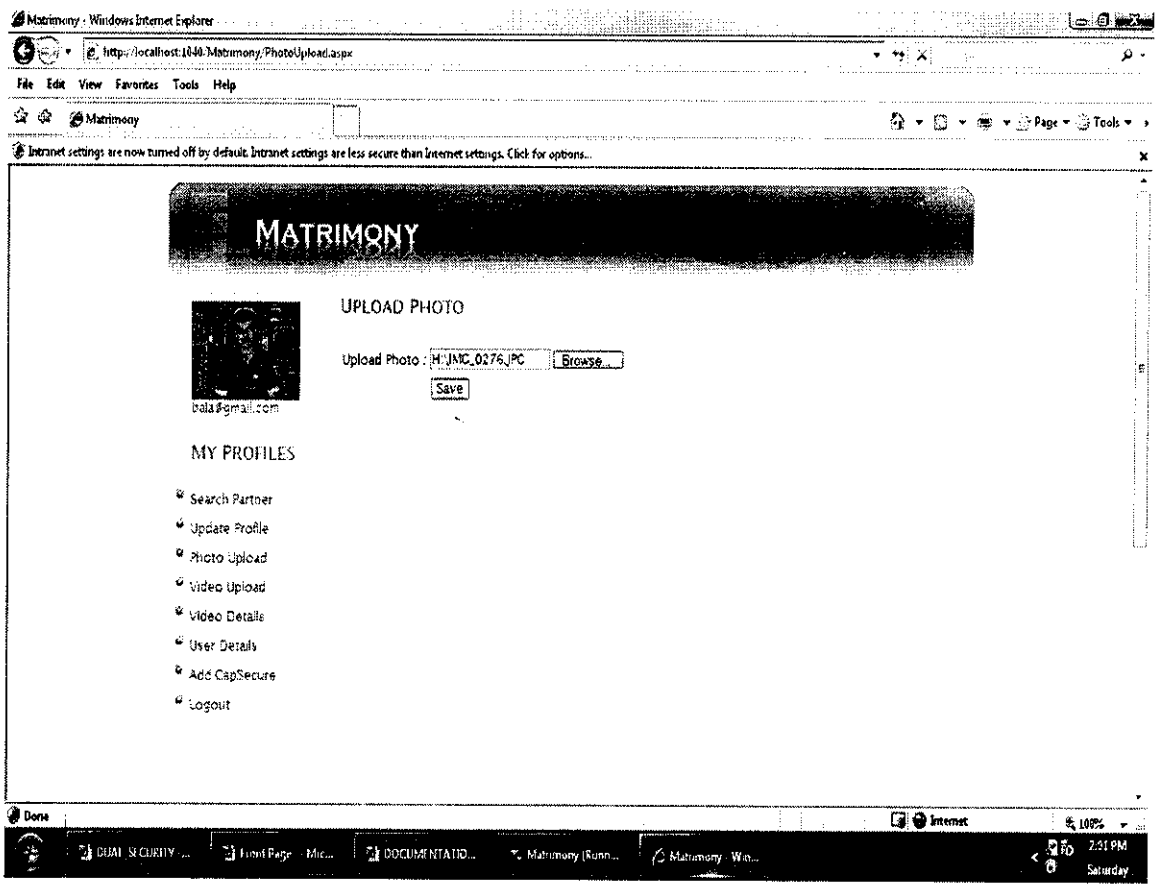
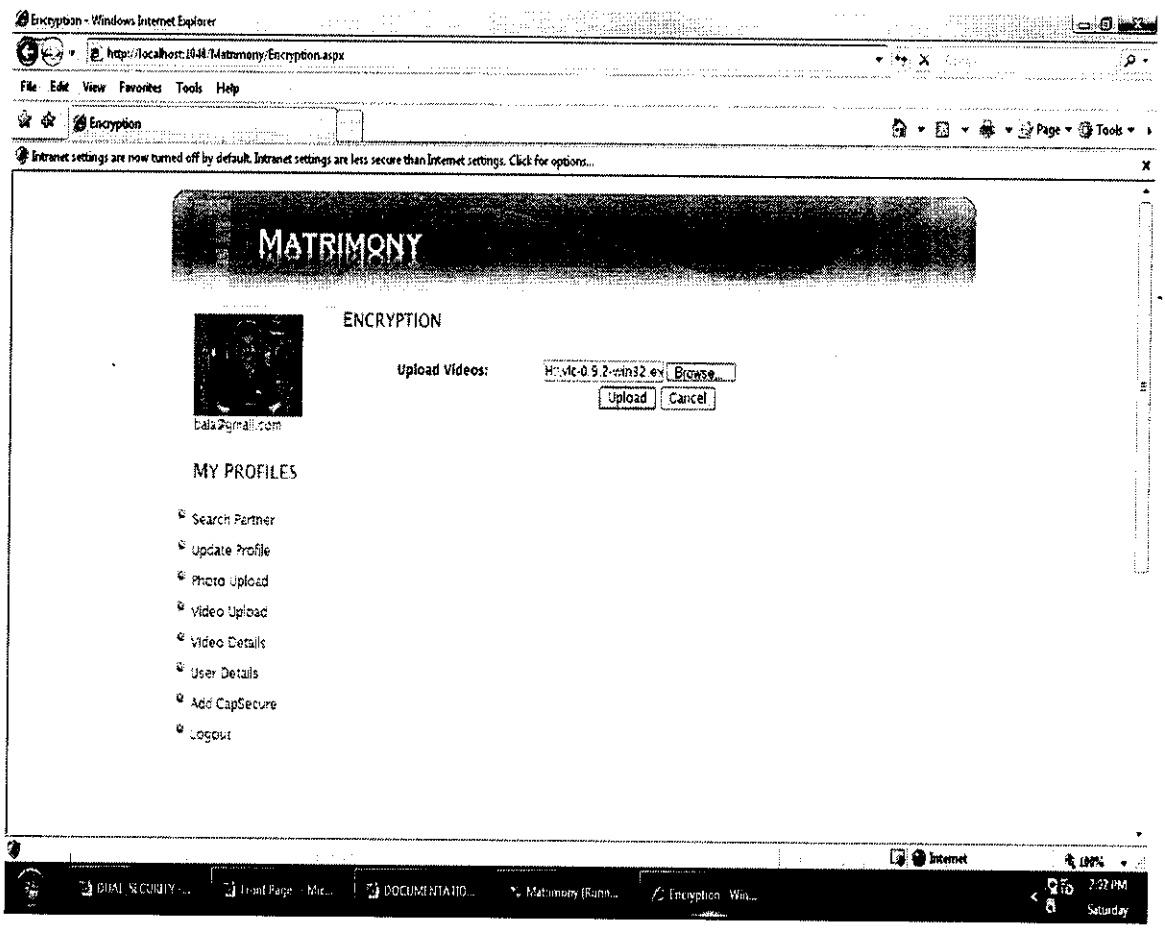


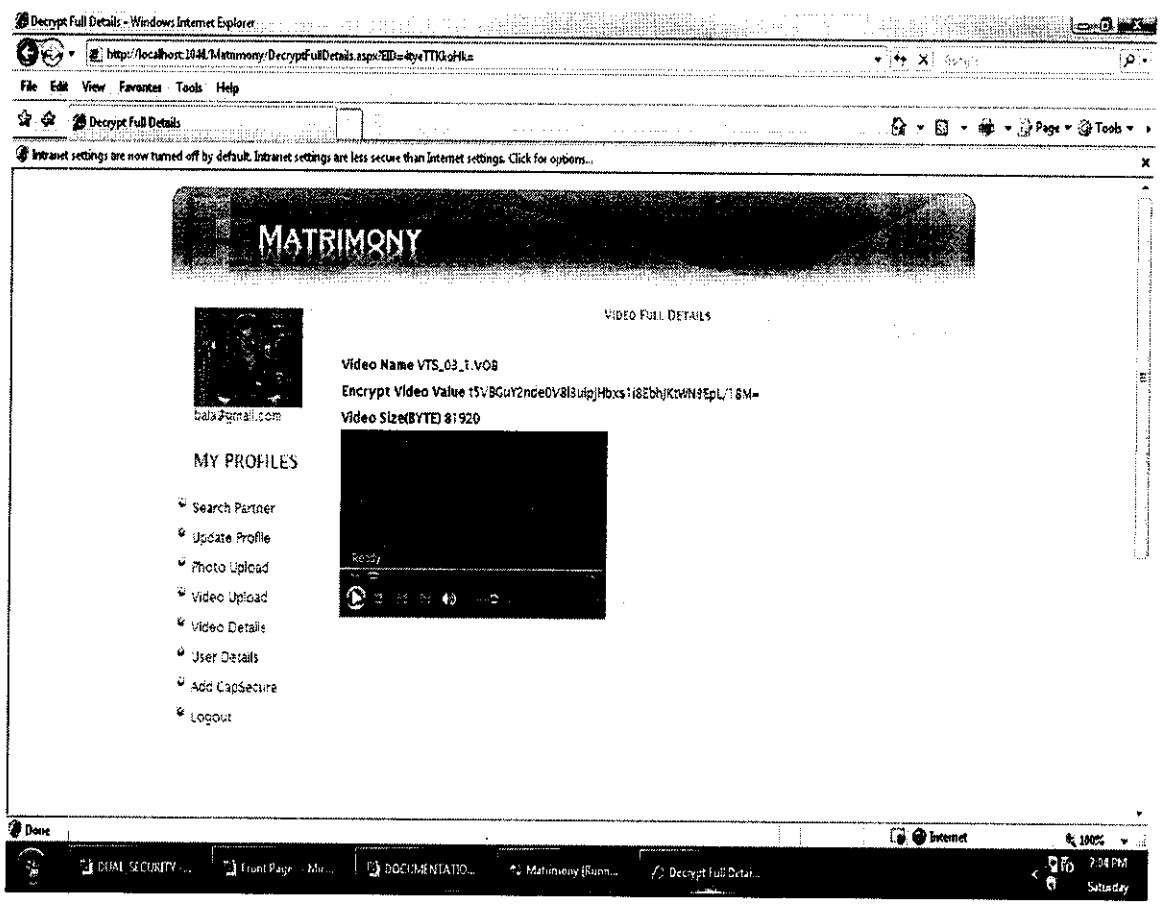
PHOTO UPLOAD



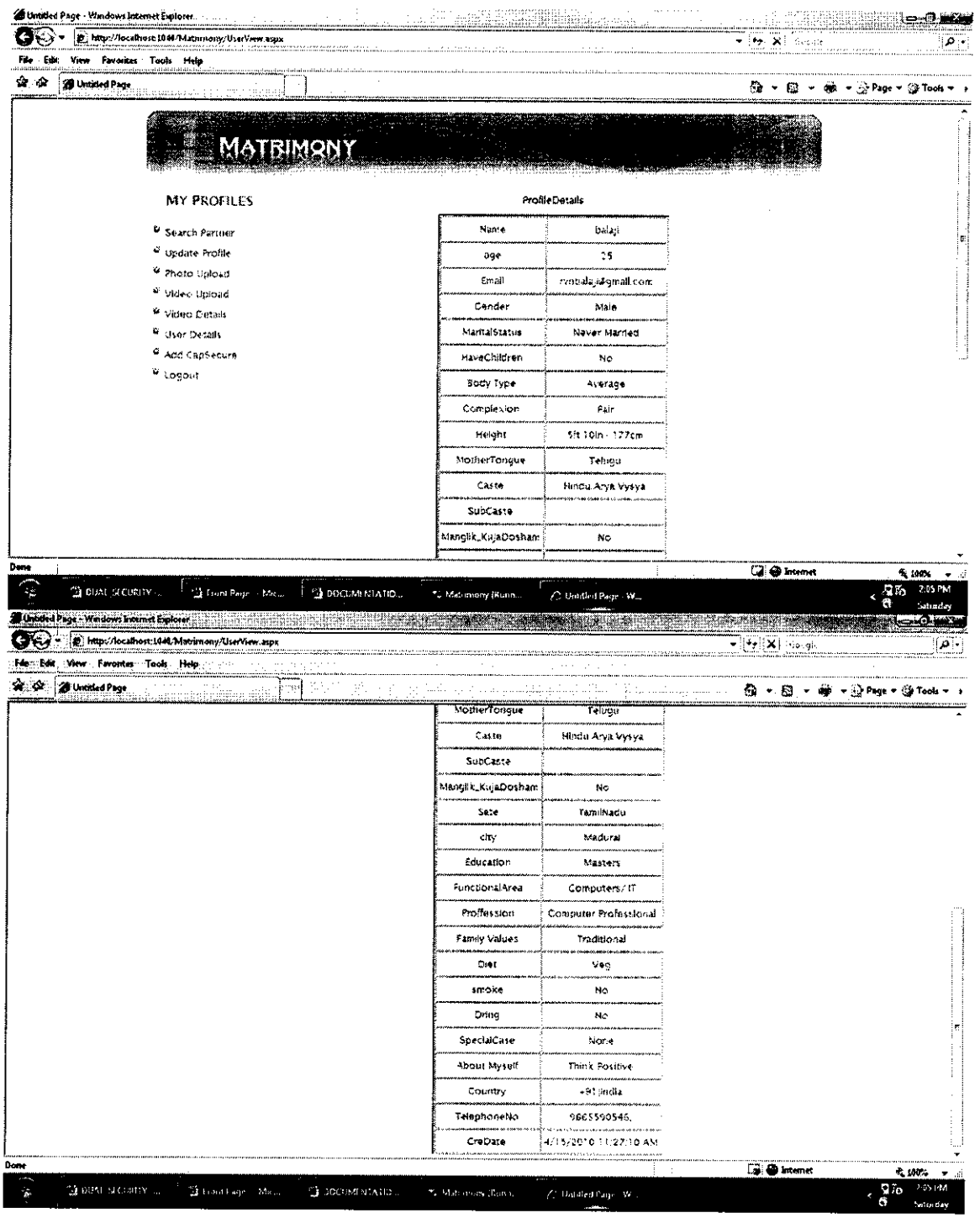
VIDEO UPLOAD



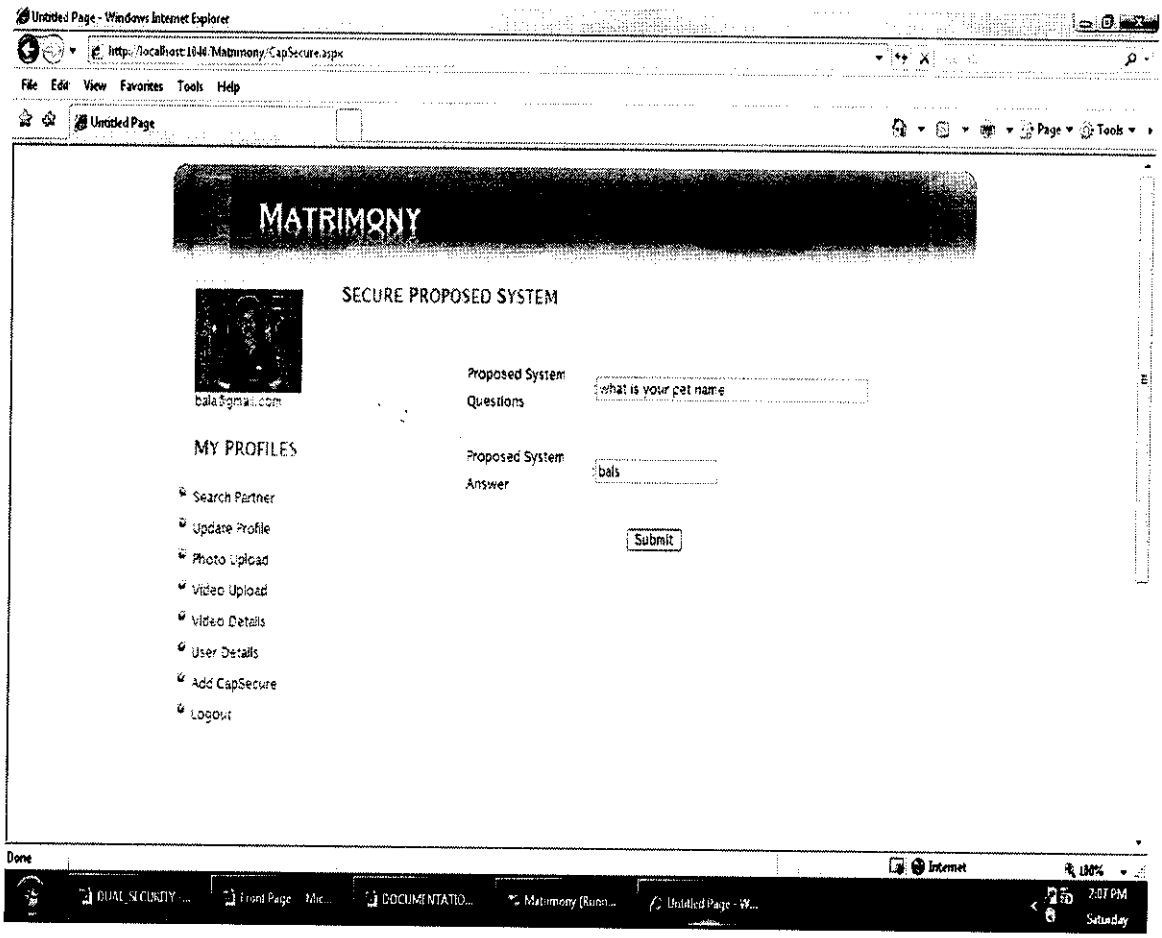
VIDEO DETAILS



USER DETAILS



CAPTCHA SECURE



REFERENCES

1) ".NET Framework Pofessional Projects", Angsbuman and Uday Kranti, Published by Prentice – Hall of India Private Limited , 3rd Edition 1997, Page No: 208-215

2) "ASP.NET 1.1 with Visusl C#.Net ", Chris Ullman and chris Hart, WROX Publications, 2nd Edition 2006, Page No: 659-211

3) Matthew MacDonald , "ASP.NET : The Complete Reference " .Tata Mc Graw – Hill, #rd Edition 2002, Page No: 195-225

4) Russ Basiura and Mike Clark ." Professional ASP.NET Web services" , SPD Publication, Page No: 53-84

5) Della-Libera, G., Hada, S., Hondo, M., Hallam-Baker and Simon, D. (2002), Web Services Security (WS-Security), International Business Machines Corporation, Microsoft Corporation.

ONLINE REFERENCE

www.codeguru.com

www.codeproject.net

www.timesjob.com

www.google.com

www.w3schools.com

www.dotnetspider.com

www.aspnet.com

www.projectplace.com

www.projectperfect.com