



Authentication Session Password Scheme Using Texts and Color

1st C.SURESH¹, 2nd V.VIDHYA², 3rd E.SHAML³, 4th P.MAHALAKSHMI⁴, 5th R.MUTHULAKSHMI⁵

¹B.TECH Information Technology(Final year) & Mailam Engineering College, India

²B.E Computer Science Engineering (Final year)& Mailam Engineering College, India

³B.E Computer Science Engineering (Final year)& Mailam Engineering College, India

⁴B.E Civil Engineering (Final year)& Mailam Engineering College, India

⁵B.E Computer Science Engineering (Third year)& Mailam Engineering College, India

Abstract

Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eyes dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To consider this problem, text can be combined with colors to generate session passwords for security purpose. Session passwords can be used only once and every time a new password is generated. In this paper, two techniques are proposed to generate session passwords using text and colors which are protect data from dictionary attack, shouldering etc. These methods are suitable for Personal Digital Assistants.

Keyword

Authentication , pair based , color based , passfaces , Hybrid method

1: INTRODUCTION

In this chapter, we would just briefly look into the introduction of the project requirements needed for it and its purpose and aim. Also, a simple development plan for the prototype system which was drafted out is being presented here in this chapter. An overview of the system initially planned to be developed is also being presented here.As proposed earlier, this project mainly focuses on the authentication of the user by using session passwords. For this 2 techniques are used which are

-Pair based method.

-Hybrid method.

Now the main aim of session password is that the various techniques used by an imposter to get access to the system fail.

2: EXISTING SYSTEM

1) Dhamija and Perrig:

Proposed a graphical authentication scheme in which the user identifies the pre-defined images to prove the authentication of the user. In this scheme, during registration the user selects a set of images from a predefined set of images. Later on at the login time the user has to select the images that he had selected during the registration time to prove his authentication. But this system is vulnerable to shoulder-surfing.

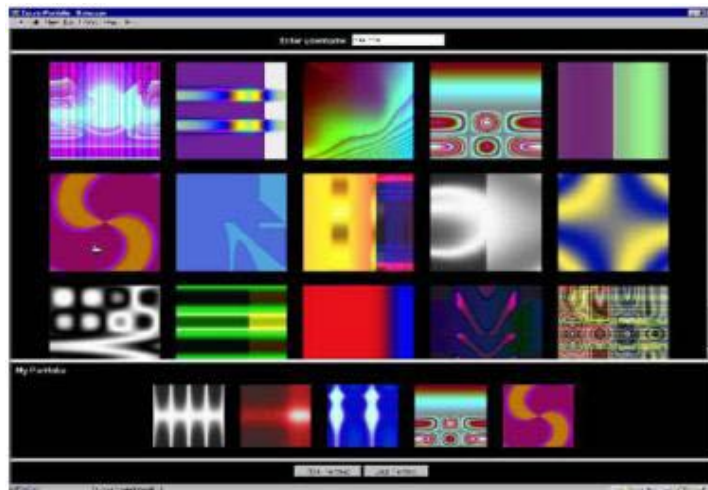


Fig no:- 2.1

2) Passfaces:

Later on a new scheme was introduced known as Passfaces. Further studies were made on authentication schemes and a new scheme was proposed known as “Draw-a-Secret” (DAS) by Jermyn, et al. The user has to draw a picture on the grid at the time of registration. The user has to draw the same picture on a 2D grid at the time of login. If the drawing of picture touches the same grid in same sequences the users gets authenticated. But this scheme was prone to shoulder surfing attacks.



Fig no. :- 2.2

3) Draw –A-Secret:

Proposed a new technique called “Draw- a-Secret” (DAS) where the user is required to redraw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.

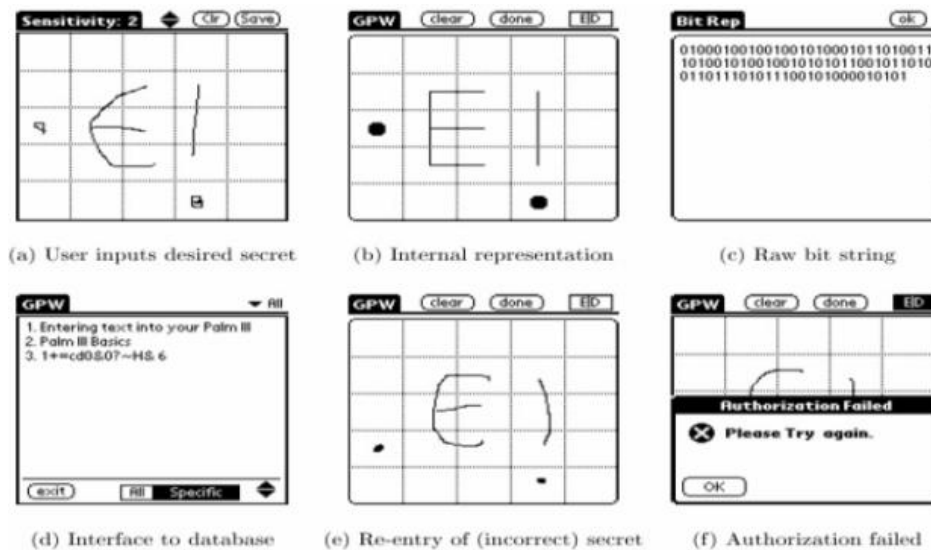


Fig no. :-2.3

4) Signature Technique:

Syukri developed a technique where authentication is done by drawing user signature using a mouse. This technique included two stages registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature.

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his/her password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface grid displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

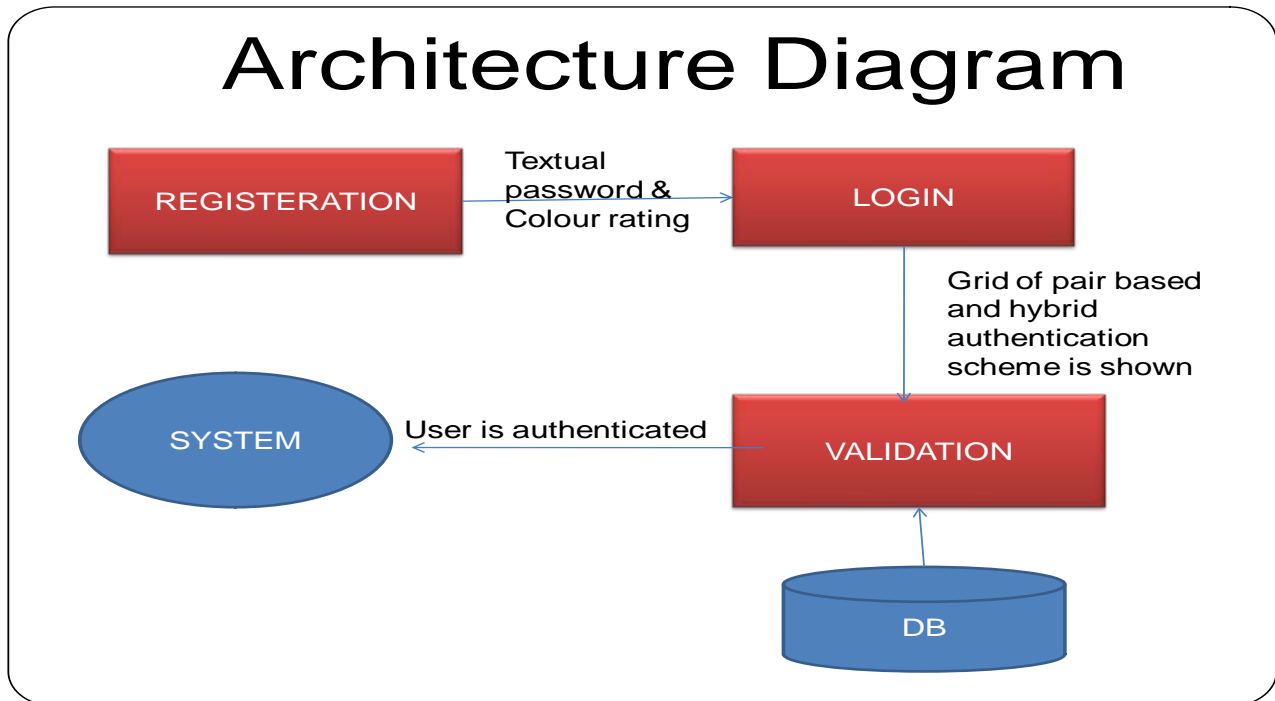


Fig. no. :- 3.1

3.1 Pair-based Authentication scheme:

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers also special symbols. These are randomly placed on the grid and the interface changes every time but new session must be generates.



Fig No:- 3.2- Pair-based Authentication login grid

User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets, digits and special symbols.



Fig No:- 3.3-Intersection letter for the pair AN

The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Above figure shows that L is the intersection symbol for the pair “AN”. The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is

allowed to enter in to the system. The grid size can be increased to include special characters in the password.

3.2 Hybrid Textual Authentication Scheme:

During registration, user should rate colors as shown below. The User should rate colors from 1 to 4 .Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. So based on the registered ratings, we have set the ratings for this color pattern which is displayed during login time. This newly given rating is called as **rated password**.

3	4	1	2

Fig No:- 3.4-Colour grid

The login interface consists of grid of size 4 x 4. This grid contains digits 1-4 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 2 pairs of colors. Each pair of color represents the row and the column of the grid.

	1	2	3	4
1	3	4	2	1
2	2	1	3	4
3	1	2	4	3
4	4	3	1	2

Fig No:- 3.5-Colour matrix during login phase.

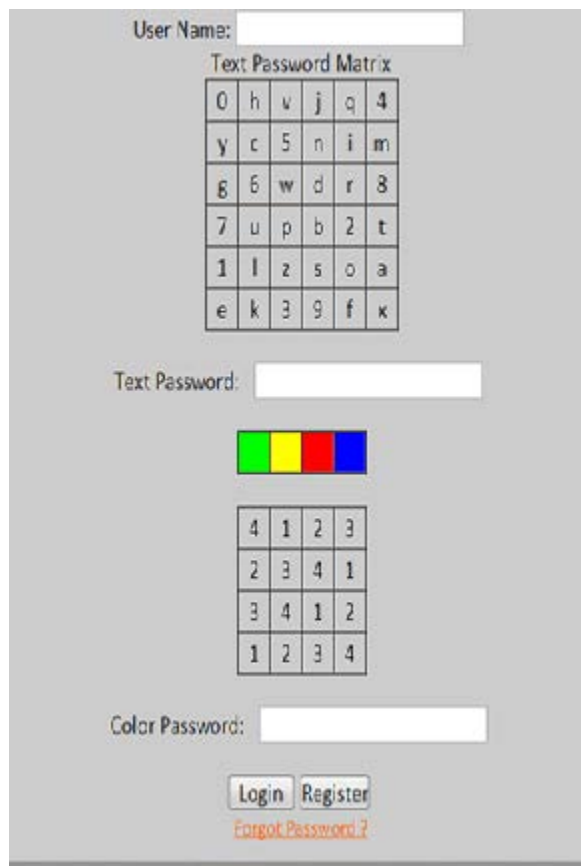
Once we have rated the colors, the next step is to divide the ratings into a pair of two such that first digit is row element and the second digit is the column element. The intersection of these two elements is the session password.

So, in our example, the rated password 3412 is broken into a pair of two as 34 and 12.

Now, as per previous statements, 3 is the row element and 4 is the column element. Now, we will search for the intersection element for 3 and 4 in the above color matrix. After searching, we get 3 as intersection digit which is the session password for 34. Likewise, we will generate session password for the remaining pairs. Hence, for another pair i.e. 12, we get 4 as session password.

Thus, by combining, we get final session password as **34** for rated password “**3412**”. Finally, both the session passwords i.e. one obtained in textual authentication scheme and another in color authentication scheme are checked at the server side. If it corrects then the user is allowed to access the particular homepage or system.

3.3 Combined system:



The screenshot shows a login form with the following elements:

- User Name:
- Text Password Matrix:

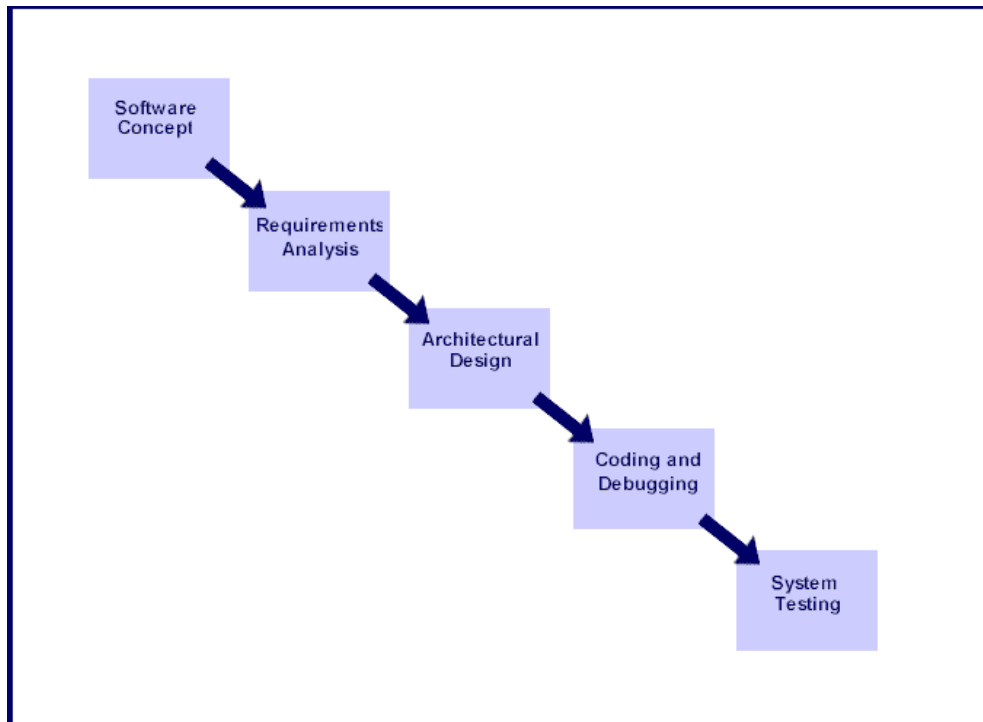
0	h	v	j	q	4
y	c	5	n	i	m
g	6	w	d	r	8
7	u	p	b	2	t
1	l	z	s	o	a
e	k	3	9	f	x
- Text Password:
- Color Password: A row of four colored squares (Green, Yellow, Red, Blue).
- Color Password Matrix:

4	1	2	3
2	3	4	1
3	4	1	2
1	2	3	4
- Color Password:
- Buttons: Login, Register, [Forgot Password?](#)

Fig No:- 7.6

4: METHODOLOGY

This project will be built on the waterfall mode. This model suggests work cascading from step to step like a series of waterfalls. It consists of the following steps in the following manner.



- **Steps involved in the System Development Life Cycle :**

Below are the steps involved in the System Development Life Cycle. Each phase within the overall cycle may be made up of several steps.

Step 1: Software Concept

The first step is to identify a need for the new system. This will include determining whether a business problem or opportunity exists, conducting a feasibility study to determine if the proposed solution is cost effective, and developing a project plan.

This process may involve end users who come up with an idea for improving their work. Ideally, the process occurs in tandem with a review of the organization's strategic plan to ensure that IT is being used to help the organization achieve its strategic objectives. Management may need to approve concept ideas before any money is budgeted for its development.

Step 2: Requirements Analysis



Requirements analysis is the process of analyzing the information needs of the end users, the organizational environment, and any system presently being used, developing the functional requirements of a system that can meet the needs of the users. Also, the requirements should be recorded in a document, email, user interface storyboard, executable prototype, or some other form. The requirements documentation should be referred to throughout the rest of the system development process to ensure the developing project aligns with user needs and requirements.

Professionals must involve end users in this process to ensure that the new system will function adequately and meets their needs and expectations.

Step 3: Architectural Design

After the requirements have been determined, the necessary specifications for the hardware, software, people, and data resources, and the information products that will satisfy the functional requirements of the proposed system can be determined. The design will serve as a blueprint for the system and helps detect problems before these errors or problems are built into the final system. Professionals create the system design, but must review their work with the users to ensure the design meets users' needs.

Step 4: Coding and Debugging

Coding and debugging is the act of creating the final system. This step is done by software developer.

Step 5: System Testing

The system must be tested to evaluate its actual functionality in relation to expected or intended functionality. Some other issues to consider during this stage would be converting old data into the new system and training employees to use the new system. End users will be key in determining whether the developed system meets the intended requirements, and the extent to which the system is actually used.

Step 6: Maintenance

Inevitably the system will need maintenance. Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly

affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

4: REQUIREMENT GATHERING AND PLANNING

4.1 Requirement Elicitation

4.1.1 Use Case Diagram and description

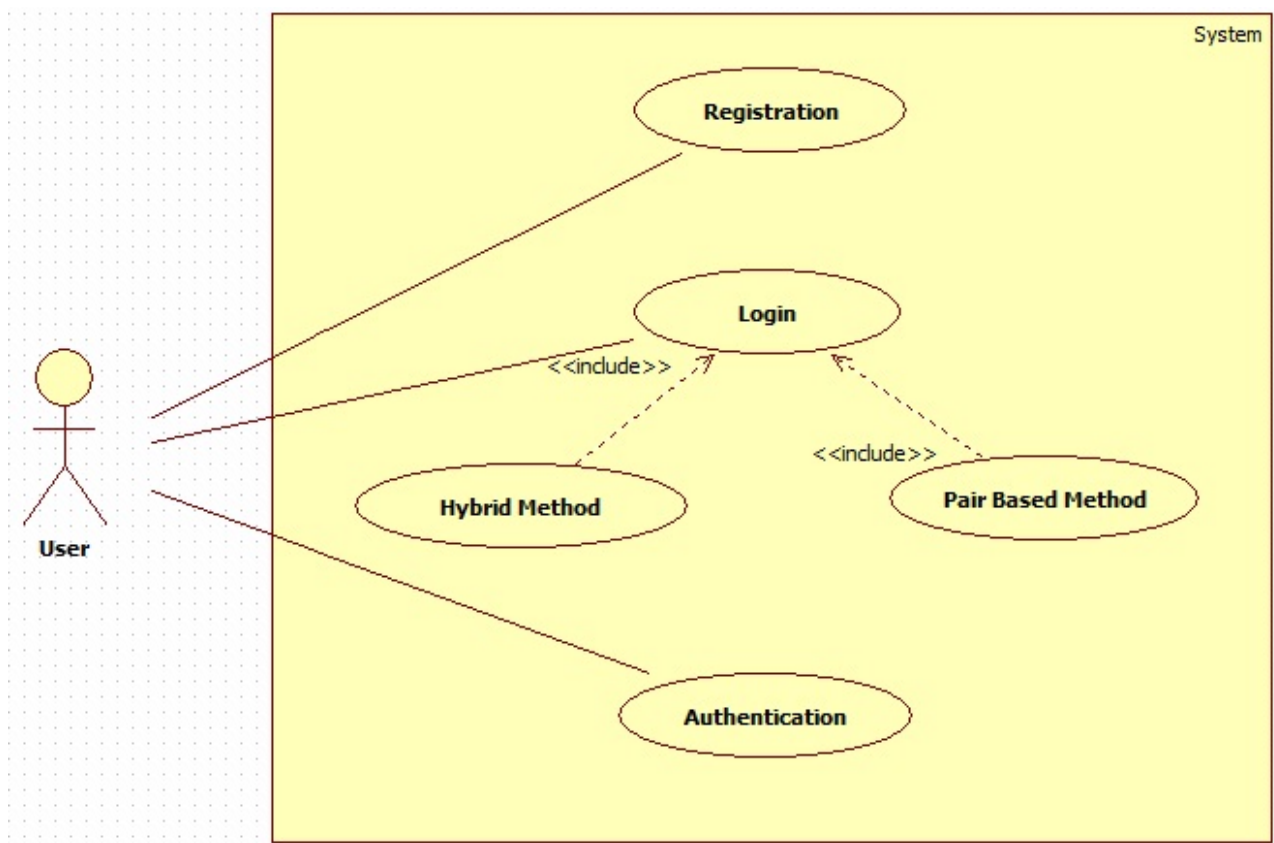


Fig No:- 4.1-Use Case

SR.NO	ACTORS	USE CASE DESCRIPTION
1	User	<ul style="list-style-type: none"> Enters User id Enters Session password.



4.2 FEASIBILITY STUDY

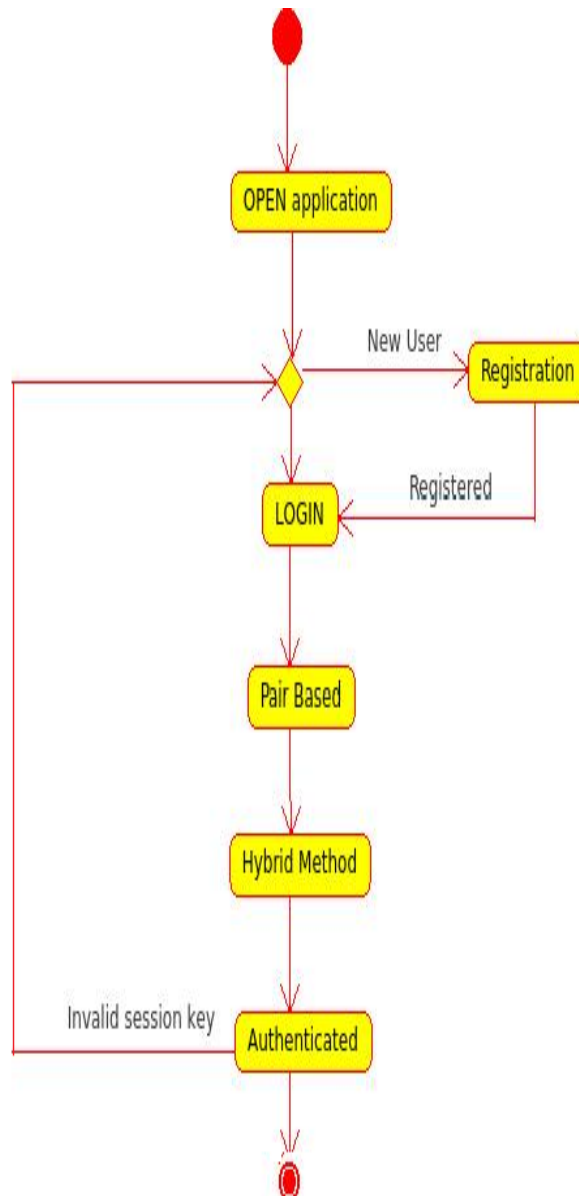
The very first phase in any system developing life cycle is preliminary investigation. The feasibility study is a major part of this phase. A measure of how beneficial or practical the development of any information system would be to the organization is the feasibility study.

5: ECONOMICAL FEASIBILITY

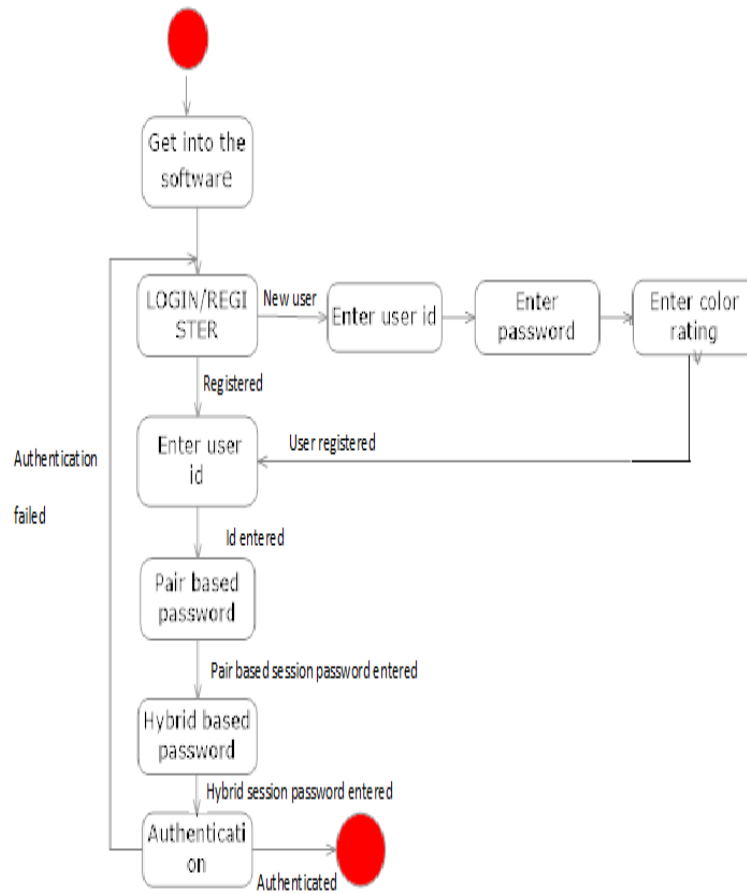
- Once the hardware and software requirements get fulfilled, there is no need for the user of our system to spend for any additional overhead.
- For the user, the web site will be economically feasible in the following aspects.
 - The normal textual passwords authentication systems are free. Whereas, this authentication system is free as well as more secure.
 - The storage and handling problems of this system will not require any third party software.

6: ANALYSIS

10.1 Activity Diagram



10.2 State Diagram

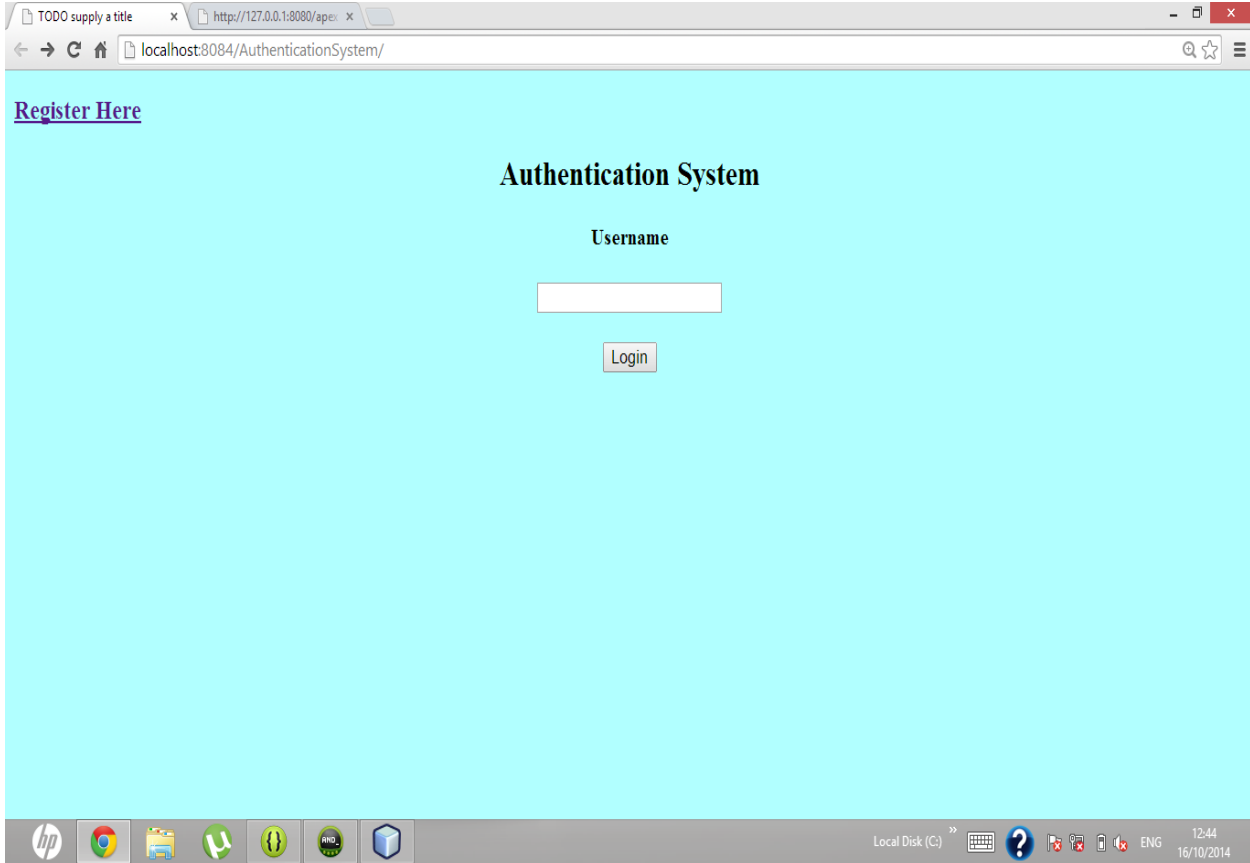


7: DESIGN

7.1 UI Design



1) Home Page



2) REGISTRATION PHASE



Enter Details

Name

Email

Address

Mobile

Password

1. 2. 3. 4.

Colour-Rating



REFERENCES

- [1] VAISHNAVI PANCHAL, CHANDAN P. PATIL a user study using “Authentication schemes for session password” March 2013.
- [2] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini “authentication technique for engg session passwords with colors” 2012.
- [3] Jermyn, I., Mayer A., Monroe, F., Reiter, M., and Rubin., “Thedesign and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.
- [4] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996