ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

# Multilevel Authentication System

[1] Nichita Silva Lobo, [2] Beverly Rodrigues [3]Pavni Alluri [4]Prathibha Singh [5]Nicole Alvares
[6]Beverly Menezes [7]Asst Prof. Amey J. Shenvi Khandeparkar [8] Asst Prof. Sneha Hazare.
[1]-[7] Department of Computer Science
Padre Conceicao College of Engineering Verna, India

***Abstract*— Textual are the most simple to use and implement. They are the most common method used for authentication but are also vulnerable to spyware key, loggers, eves dropping and dictionary attacks. To address this problem and make the system more secure this paper proposes three different levels of authentication namely textual passwords, pair-based password and graphical password. Combining all the three level this paper focuses on providing the user with stronger security and a user friendly interface.**

***Keywords*—Authentication, multilevel security, passwords, textual passwords, pair-based session passwords, graphical passwords.**

## I. INTRODUCTION

Authentication refers to the act of approving the users identity. Textual passwords are the most conventional type of user authentication systems used. Textual passwords should be easy enough for the user to remember and hard enough for the attacker to guess. Users normally select short and easily guessable passwords which are frequently targeted using brute force and dictionary attacks. Imposing a strong passwords policy can be a solution to this problem but since these passwords are tough to remember users tend to write the password down, disclosing them to direct theft. Other flaws include vulnerability to shoulder surfacing and key loggers.

We need a unique and user friendly authentication to make passwords more secure and reliable. New techniques like graphical passwords, OTPs and biometric passwords are being developed. The development of internet and WWW requires us to have more secure approaches then the usual text based security systems, therefore this demands the need for something more secure as well as user friendly. Hence, we have tried to increase the security by using a three level security mechanism.
In this paper, we are using three different authentication schemes which when combined together will provide the user with a highly secure system.

## II. PROPOSED SECURE SYSTEM

This user friendly multilevel authentication system involves three levels of security. Our proposed system can be customised depending on the users preference. The user can select the number of levels required depending on how sensitive the data is. In case of a combination of levels, the preceding level must be passed in order to precede to the next level.

### *A. Level 1*

Security at level 1 has been imposed by using text based password which is a conventional password system. Users have to set a text password initially.

### *B. Level 2*

Level 2 is a pair based password where the user submits his password during the registration phase. During the login phase when the user enters his username an interface consisting of a randomly generated grid is displayed.The user enters his password based on this grid. The system veriifes the passord entered by comparing with the password saved during registration.

### *C. Level 3*

Level 3 is imposed by a graphical password system. In this system the user can select a sequence of desired images into the system and then create a password by clicking on a single point on each image. During the login process the user has to select click points in the saved sequence.

## III. SYSTEM DEDIGN

Our system design consists of 4 modules:- Textual password module, pair-based password module, graphical password module and retrieval module.

### *1) Textual password module*

In the first level the textual password approach is used along with converting the text based password to a bipolar form. The first level consists of two phases mainly the registration phase and a login phase.

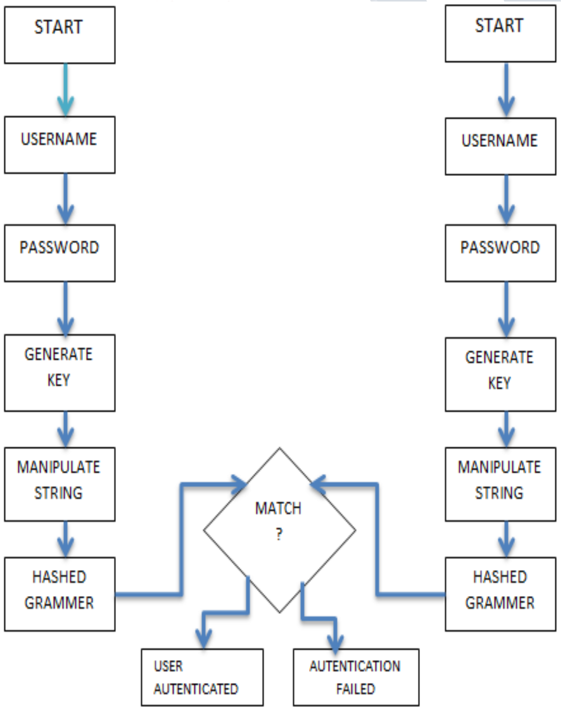
During registration phase the user enters the username and password. The password should be of minimum 7 characters and maximum 12 characters. The username and the password are concatenated to obtain a string from which a key is then generated. The key is generated using the following formula:

Key= (sum of the ASCII values of all letters in the string)mod4.

Where 4 indicates the four string manipulation techniques that we will use. This key is then used to manipulate the password and the string is then converted to binary and then to bipolar form and store to the database along with the username.

During login phase the user name enters the username and the password anf the same procedure takes place. Finally, the password obtained in bipolar form is compared with the previously stored password. The user is authenticated is both match, else a failure message is displayed.

*Fig: Flow of textua*



*l password module*

### *2) Pair – based password module*

The pair based authentication scheme is used for generating session passwords for the stored password. During the registration phase, username and password is accepted as shown in the figure.

Bipolar form of this password and username is then store into the database. During login phase, instead of the stored password, the entered session password is used for authenticating the user.

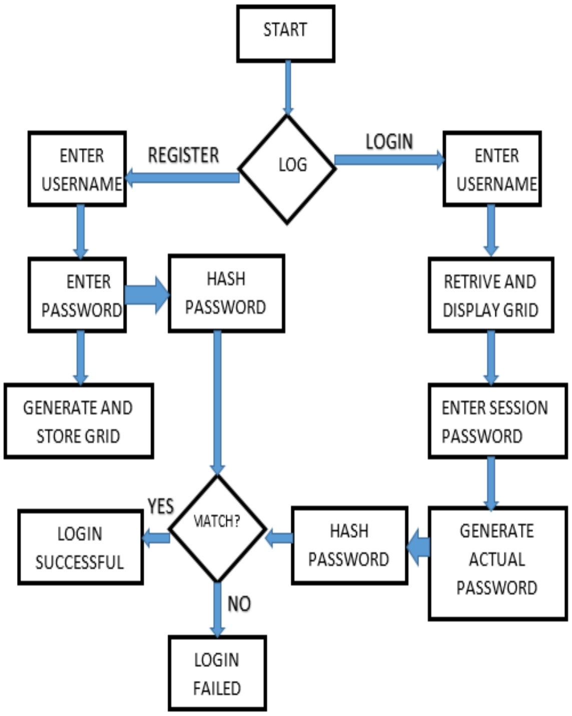


*Fig: Flow of Pair Based Password Module*

If the user opted for this level of authentication, a 6x6 grid containing all 26 characters and 0-9 numbers is displayed. This grid changes randomly for each login session. Now according to the stored password, the user has to enter the session password in the grid.

The session password for a character in the secret key is any character from its row n and any character from its column respectively. The figure shows a pair-based password grid. According to the grid shown in the figure, the session password for character 'p' in the secret key can be 'gy', '4q','0n' etc.

| | | | | | |
|---|---|---|---|---|---|
| a | q | 6 | j | 7 | x |
| r | y | f | 3 | e | i |
| g | p | 4 | u | 0 | s |
| 5 | w | b | h | d | 2 |
| o | m | v | 8 | l | t |
| z | n | 9 | c | 1 | k |

*Fig: Randomly Generated Pair Based Password Grid*.

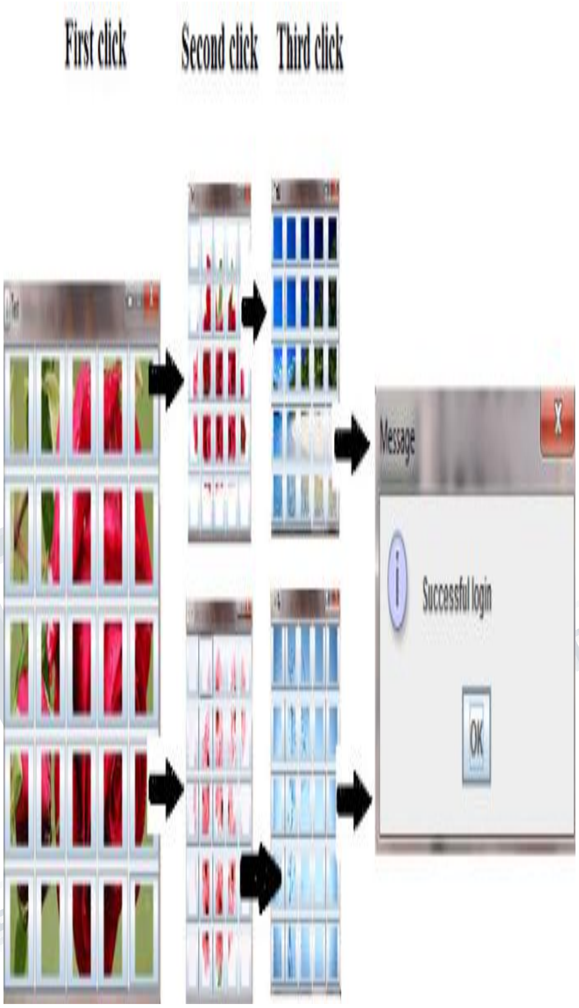
So, basically the intersection of the row of the first character and the column of the second character in the pair of characters of the session password should match with the corresponding character of the stored password for the user to get authenticated. In case, the intersection doesn't match with the corresponding stored character, an authentication failure message is displayed.

### 3) *Graphical password module*

The third level is a graphical password module, for graphical module we are using the cued click points authentication technique. There are two phases: registration phase and login phase. During registration phase, the user will have to choose 5 images in a particular sequence for the image pool given by the system.

For each image he or she will have to choose a distinct point. Some amount of tolerance is accepted, that is, the user is allowed to click on any point falling within the specified range of the original clicked point. This point in the In the image will take him to the next image. Hence, in this approach the password is the sequence of images and the point on each image.

While logging in, the first image is displayed and the user will have to select the correct click point on that image. If the selected point on that image is correct, only then the next image of the original sequence will be shown. If the clicked point is wrong, then any random image will be shown in screen leading to an incorrect sequence. The figure shows how a wrong click point leads to a formation of random sequence of images.



Successful login

*Fig. Cued Click Point Authentication Technique*

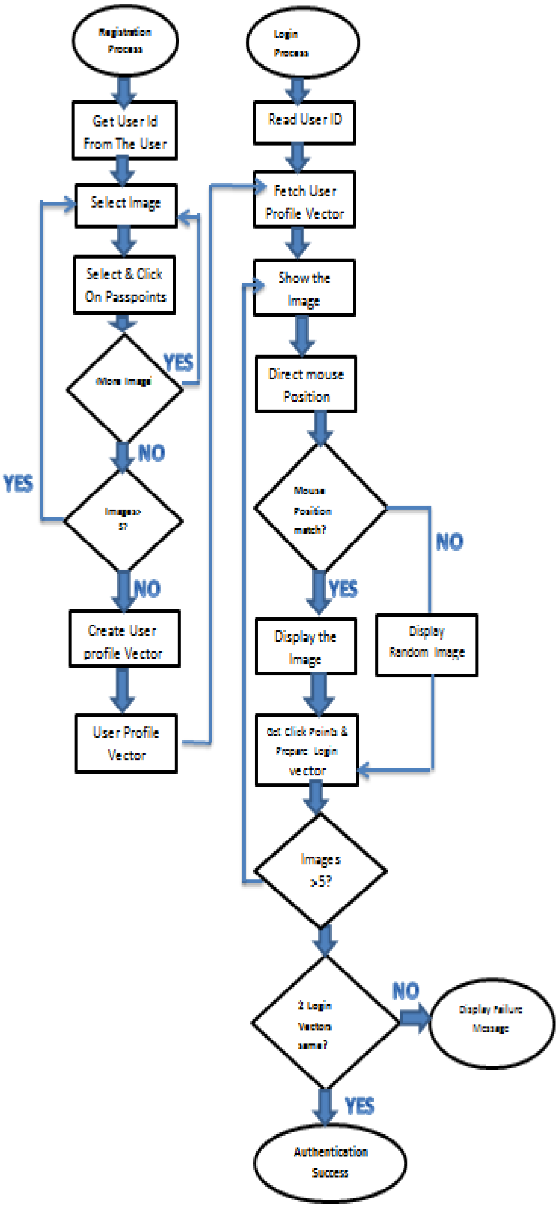


*Fig: Flow of Graphical Password Module*

So if the images are not according to the original sequence, the user will come to know that he has clicked on the wrong point. The tolerance level is defined by the grid shown on the image selected by the user during registration. Each point on the image has a tolerance of one block. This implies that during login phase, a user clicking within the block of the correct points is authenticated. The message of authentication failure is shown at the end when all the five points are chosen. Hence, if someone other than the user is trying to get authentication then he won't know on with image he made a mistake.

### 4) *Resetting password module*

Resetting module plays an important role in our system since it has to provide security as strong as provided by all the three levels of our authentication system. It has to be strict enough to prevent hackers from accessing the system. Resetting module is invoked when a user may have been locked out when he forgets his password or Login ids are disabled due to several number of invalid attempts made by a hacker or user.

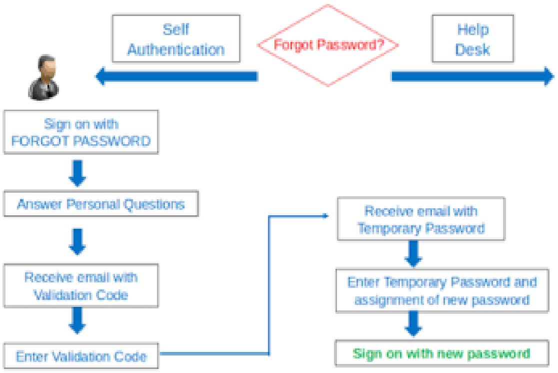
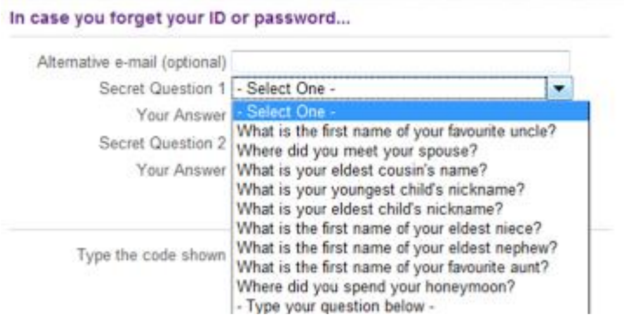

Self Authentication
Forgot Password?
Help Desk
Sign on with FORGOT PASSWORD
Answer Personal Questions
Receive email with Validation Code
Enter Validation Code
Receive email with Temporary Password
Enter Temporary Password and assignment of new password
Sign on with new password

*Fig: Flow of Retrieval Module.*

The job of the resetting module is to help the user when he forgets the password or username. During registration phase, after entering all his details in the registration form he needs to enter few security questions and answer for the same.

In case a user forgets his password he can access those security questions and answer them. On answering correctly the user will be allowed to reset the password. User is exposed to maximum 3 attempts. A timer is set when user exceeds 3 attempts and is not allowed to reset for next 1 hour preventing the system from hacking.


In case you forget your ID or password...

Alternative e-mail (optional)
Secret Question 1 - Select One -
Your Answer
Secret Question 2
Your Answer
Type the code shown

- Select One -
What is the first name of your favourite uncle?
Where did you meet your spouse?
What is your eldest cousin's name?
What is your youngest child's nickname?
What is your eldest child's nickname?
What is the first name of your eldest niece?
What is the first name of your eldest nephew?
What is the first name of your favourite aunt?
Where did you spend your honeymoon?
- Type your question below -

*Fig: Security Question Interface.*

## IV. KEY CONSIDERATIONS

### TOLERANCE

In our system the tolerance level is defined by the grid shown in the image selected by the user during registration. Each point in the image is having a tolerance of 1 block. This implies that during login phase a user clicking within the clicks of the correct points is authenticated.

### *IMAGE*

Images that are provided by the system to the user are properly chosen such that there are no hotspots in that image.

### *TEXTUAL PASSWORD SELECTION*

Textual passwords that a user enters into the first and the second level has to be if minimum 7 characters and maximum 12 characters.

### *SECURITY QUESTIONS*

Security questions are to be answered in order to reset the password. We allow user to set those security questions. While setting the security question user need to keep in mind that the hacker will try to enter into the system through resetting module hence he can add questions whose answers are not known to others.

## REFERENCES

1) Nagesh D. Kamble, J. Dharani "Implementation of Security System Using 3-Level Authentication" (IJEDR)(Volume 2, Issue 2,2014)

2) M Sreelatha, M Shashi, M Anirudh, Md Sultan Ahamer, V Manoj Kumar, "Authentication schemes for Session Passwords using Color and Images", International Journal of network Security and Its Applications" (IJNSA),(volume 3, No.3, May 2011)

3) Iran a a m, PankajaPatil, "Graphical Password Authentication using Persuasive Cues Click Point" International Journal of Advanced Research in Electrical, Electronics and Instrumental Engineering (Vol.2 Issue 7,July 2013)

4) Kunal Mulwani, SaurabhNaik, Navin Kumar Guarnani, Dr. Nupur Giri, Prof. SharmilaSengupta, "3LAS(Three Level Authentication Scheme)" International Journal of Engineering Technology and Advanced Engineering ( ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 8, August 2013)