Graphical Password Authentication

Prathmesh More[1] Rahul Mundhe[2] Jayesh Tribhuvan[3] Pratap Nair[4]
[1]Engineering Student, [2]Engineering Student, [3]Engineering Student, [4]Assistant Professor
[1]Computer Engineering Department,
[1]K. C. College of Engineering and Management Studies and Research, Mumbai, India

Abstract : For Authentication,Textual passwords are widely used. But they are vulnerable to different attacks like dictionary attacks,eves dropping,shoulder surfing.So, for text password there is alternative method referred as Graphical passwords.In this paper,two methods are implemented to generate session passwords using colors and text.

IndexTerms – **Authentication,Pair-Based,Hybrid-Textual,Registration**

INTRODUCTION

Textual passwords are mostly used for authentication of particular system. but, they are vulnerable to different attacks. lengthy and Random passwords improves the security of the system. textual passwords are easy to remember. Unfortunately, textual passwords can be easily guessed.graphical passwords more secure method for system.there different techniques used in graphical passwords.In this paper,graphical passwords are used with session password for more security.session password provide security against various attacks as password changes every session.

I. LITERATURE SURVEY

[1] Sonia Chiasson & P.C. van Oorschot, "Graphical Password Authentication Using Cued Click Points",2012:

In this scheme the user must click on the approximate areas of pre-defined points or locations. Extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity.
the user is required to draw a curve across their password images orderly rather than clicking on them directly.

[2] Miss. Swati tidke & Miss. Nagama Khan, "Password Authentication Using Text and Colors", 2015:

Introduced a session password scheme in which the passwords are used only once for each session and when session is completed the password is no longer in use. The proposed session password scheme uses
colors and text for generating session password.

[3] Mr. Umesh M. Korade & Mr.Chetan P. Shitole, "Authentication Scheme for Session Password using matrix Colour and Text", 2014:

Introduced DAS(Draw-a-secret) method is in which user is required to re-draw the image on 2-D grid. If the drawing matches the same grids in a same sequence, then the user is authenticated.

II. SYSTEM DESIGN

The Proposed system has 3 phases: registration, login and verification.During registration phase,User enters his password in first method or numbered the colors in second method,then in login phase,the user has to put the password on the screen. The system checks the password entered by comparing with the password generated during registration process.
The proposed system consists of three modules:

a. Pair-based Authentication
b. Hybrid Textual Authentication
c. Registration

The proposed authentication system works as follows:

In Hybrid textual method,User should get colors from 1 to 8 and he can remember it as “RLYOBGIP”. Same rating can be given to different colors. During login process,when user enters his username,a grid is displayed based on the colors selected by a user.

The login phase consists of 8×8 grid. This grid contains cells which can be numbered from 1-8 randomly.The interface consists strips of colors. The color grid consists of 2 pairs of colors.

In Pair-Based scheme,During registration user submits the password. Maximum length of the password is 8 number of characters and it can be called as secret pass. This pass should contain even number of characters. Session passwords are generated depending upon this pass.

During the login process, when user enters his username the 6 x 6 sized grid is displayed and it consists of alphabets from A-Z and numbers from 0-9.These are placed on the grid randomly and this grid changes on every session.

User has to enter password depending upon the secret pass.The session password consists of alphabets and digits. The first letter in the pair is represent the row and the second letter is used to represent the column.The intersection of these two letters is part of session password. This is repeated for all pairs of secret pass.

System Sequence Diagram:

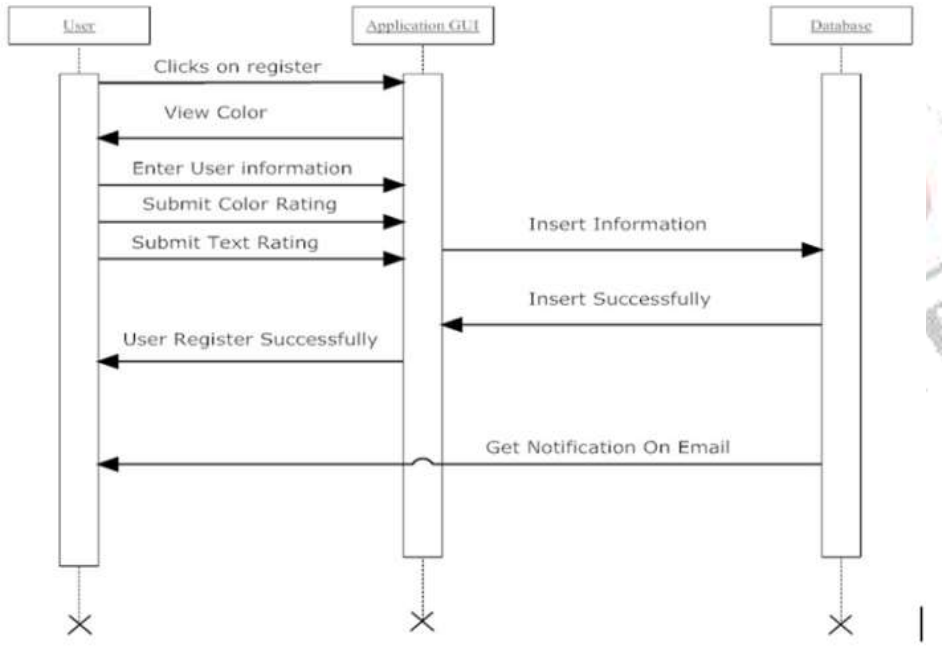

Figure 1: System Sequence Diagram

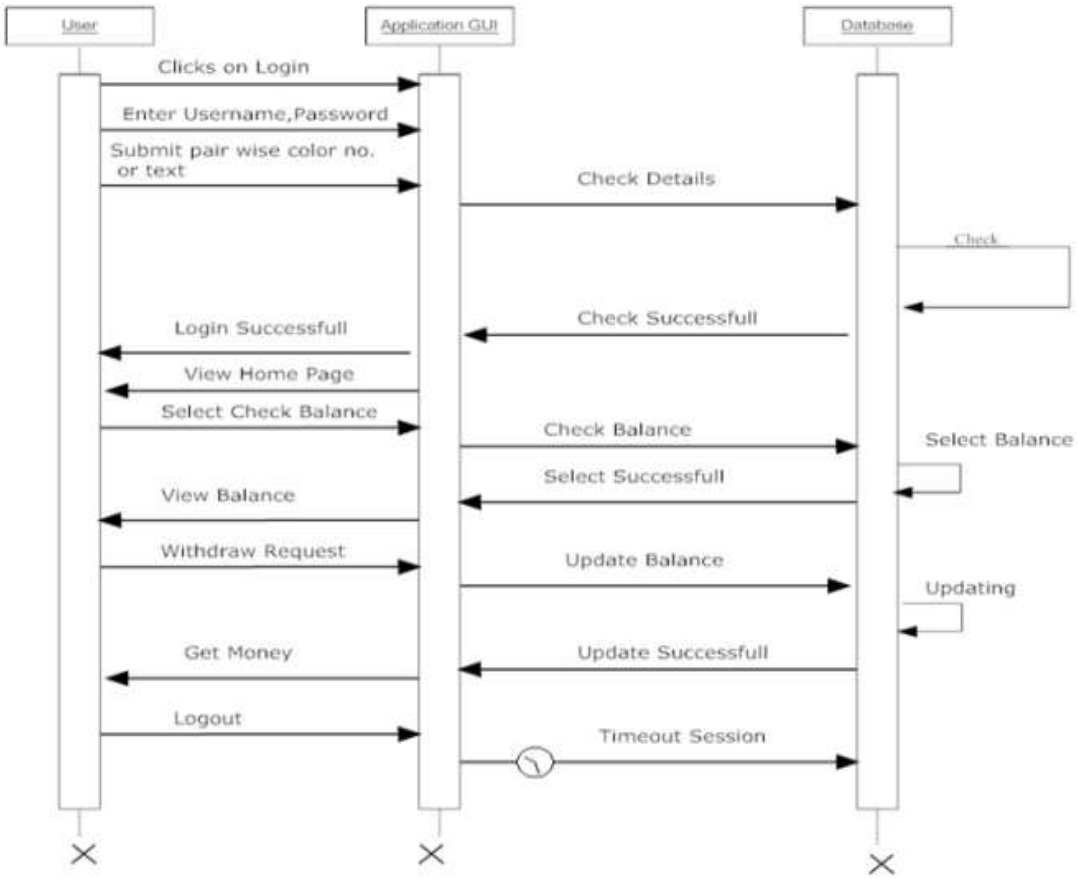

Figure 2: System Sequence Diagram

III. Applications

The following are the applications of the project:

1. Military :

It is useful for military system for securing confidential data and information.

2. Banking :

It will also be used for secure transaction of money and the useful data such as OTP, bank details of the customer.also it will be used for ATM machines

IV. Acknowledgement

We wish to express our deep sense of gratitude to our Project Guide Prof. Pratap Nair for guiding us for the project. We sincerely acknowledge for giving their valuable guidance and critical reviews and comments.
Finally, we would like to express our heartfelt thanks to all supporting staff members and friends who have been a constant source of encouragement for completion of the project.

V. Conclusion

In this Project,Text and colors are two authentication techniques are proposed. These techniques are used avoid dictionary attack, brute force attack and shoulder-surfing and other various attacks. Both the techniques use grid format for session passwords.
Pair based technique requires no special type of registration, during login time based on the grid displayed a session password is generated.
For hybrid textual scheme,number from 1-8 should be given to colors, based on these numbering and the grid displayed during login, session passwords are generated.
these techniques should be verified extensively for usability and effectiveness and they are completely new to the user

VII. References

1)R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.
2)Real User Corporation: Passfaces. www.passfaces.com.
3)A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.