International Journal of Engineering &Technology, 7 (1.7) (2018) 169-174

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A shoulder surfing resistance using graphical authentication system

Rupavathy.N[1]*, Carmel Mary Belinda M. J.[2], Nivedhitha.G[3]

[1]*Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu - 600062*
[2]*Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu - 600062*
[3]*Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu - 600062*
**E-mail :rupavathy@veltech.edu.in*

Abstract

Authentication supported passwords is employed mostly in applications for laptop security and privacy. However, human actions like selecting unhealthy passwords and inputting passwords in an insecure approach are considered "the weakest link" within the authentication chain. Instead of impulsive alphanumerical strings, users tend to decide on passwords either short or purposeful for simple learning. With internet applications and mobile apps piling up, individuals will access these applications any time and any place with numerous devices. This evolution brings nice convenience however additionally will increase the chance of exposing passwords to shoulder surfing attacks. Attackers will observe directly or use external recording devices to gather users' credentials. To overcome this drawback, we tend to plan a unique authentication system Pass Matrix, supported graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulatory horizontal and vertical bars covering the complete scope of pass-images, Pass Matrix offers no hint for attackers to work out or slim down the password even they conduct multiple camera-based attacks. We tend to additionally enforce a Pass Matrix image on android and applied real user experiments to judge its memorability and usefulness. From the experimental result, the proposed system achieves higher resistance shoulder surfing attacks whereas maintaining usability.

Keywords: *Privacy, Security, Authentication, Surfing.*

1. Introduction

The main aim of this project is to propose the smart way to authenticate the user bank account through the pictorial password and by injecting the indirect pin to the system to predict the original password using temporary login indicator while login and to provide various banking features.

The user is provided with the two-optional authentication system for the user (one is the existing and another model is proposed by us). Proposed model provides the user friendly and the interactive environment for the user. The efficient and the innovative banking service provided for the authentication system. The forget password module is designed with an innovative idea. Based on idea of framing forget password questions on the user's handheld device. Blocking the user account if wrong password injected to the server frequently and intimate the user through Email and user's alternative mobile number via SMS about current location of the mobile.

2. System Description

The Existing system the users upload or select the pre-defined image that provided by the server as a password image. If user selected the image as password the server process with the image and split the password image to 7x11 grids and display all grid images to the user, and user select the single grid as a password grid for the particular image. And user upload with multiple images as user need and select the each grid as a password for an image.

And while login the user are provided with the login indicator (temporary password). The login indicator is only visible while holding the proximity sensor of the user device and the holding the screen in circle image. Now the user is provided with the login indicator, here the user now displayed with the gridded password image with movable horizontal alphabetic bar and movable vertical numeric bar. Your login indicator will be in the form of A→6. In vertical and horizontal bar the alphabets and numeric values will be mismatch in order. The user can move the bar values by using navigation keys provided bellow. By moving the user should move the value, A vertically straight to the password grid. And move value 6 horizontal straight to the password grid. And press OK the grid will be authenticated. And user provided with next image with new login indicator. User should authenticate the images till the last image provided by the user will registration.

3. Problem Definition

1. If malicious user provide the wrong password to some user's account. No steps are taken to safeguard the user accounts.
2. None of the Services provided for the application.

3. User friendliness is less when compared to our proposed work.
4. Forget password module is not yet provided.

The proposed works of the shoulder surfing resistance are:

- The user is provided with the two-optional authentication system for the user (one is the existing and another model is proposed by us).
- Proposed model provides the user friendly and the interactive environment for the user.
- The efficient and the innovative banking service provided for the authentication system
- The forget password module is designed with an innovative idea. Based on idea of framing forget password questions on the user's handheld device.
- Blocking the user account if wrong password injected to the server frequently and intimate the user through Email and user's alternative mobile number via SMS about current location of the mobile.

Our proposed idea of login gives you the user-friendly authentication system. The system provides the login indicator from the numeric values 0 to 9. Same using the proximity sensor and holding the screen using hands to see the indicator to avoid the shoulder surfing attack. After seeing the indicator the user move to the authentication activity, there the image uploaded by the user will be loaded and above the image the numeric numbers will scattered throughout the screen. If you touch the single numeric value and drag it. The whole scattered numbers will be moved with respective to the numeric value that you are dragging. You can drag any of the number and you should place your indicator on the image password position you selected during registration.

4. Module Description

- Account creation and registering your password.
- Authentication using existing graphical authentication.
- Authentication using proposed graphical authentication.
- Forget password and recovering module
- Banking services.

Account creation and registering your password:

The users register the account with providing the user information and the optional mobile number and the email to make alert about your account in some extreme cases. The users upload or select the pre-defined image that provided by the server as a password image. If user selected the image as password the server process with the image and split the password image to 7x11 grids and display all grid images to the user, and user select the single grid as a password grid for the particular image. And user upload with multiple images as user need and select the each grid as a password for an image. If you click finish your password will be stored and account will be registered.

Authentication using existing graphical authentication:

While login the user are provided with the login indicator (temporary password). The login indicator is only visible while holding the proximity sensor of the user device and the holding the screen in circle image. Now the user is provided with the login indicator, here the user now displayed with the gridded password image with movable horizontal alphabetic bar and movable vertical numeric bar. Your login indicator will be in the form of A→6. In vertical and horizontal bar the alphabets and numeric values will be mismatch in order. The user can move the bar values by using navigation keys provided bellow. By moving the user should move the value A vertically straight to the password grid. And move value 6 horizontal straight to the password grid. And press OK the grid will be authenticated. And user provided with next image and new login indicator. After completing all image authentications, if the entered is correct your services will be provided.

Authentication using proposed graphical authentication:

Our proposed idea of login gives you the user friendly authentication system. The system provides the login indicator from the numeric values 0 to 9. Using the proximity sensor and holding the screen using hands to see the indicator to avoid the shoulder surfing attack. After seeing the indicator the user move to the authentication activity, there the image uploaded by the user will be loaded and above the image the numeric numbers will scattered throughout the screen. If you touch the single numeric value and drag it. The whole scattered numbers will be moved with respective to the numeric value that you are dragging. You can drag any of the number and you should place your indicator on the image password position you selected during registration.

Forget password and recovering module:

In forget password and recovery module, we achieve this using an innovative idea of security questions about the user handset such as charging percentage in last 2 days. Have you used camera in last two days? And have you installed any of the application. We concentrate on the log files (camera, battery usage, calendar information, call log, installed applications) of the user mobile and frame the questions based on that.

Banking services:

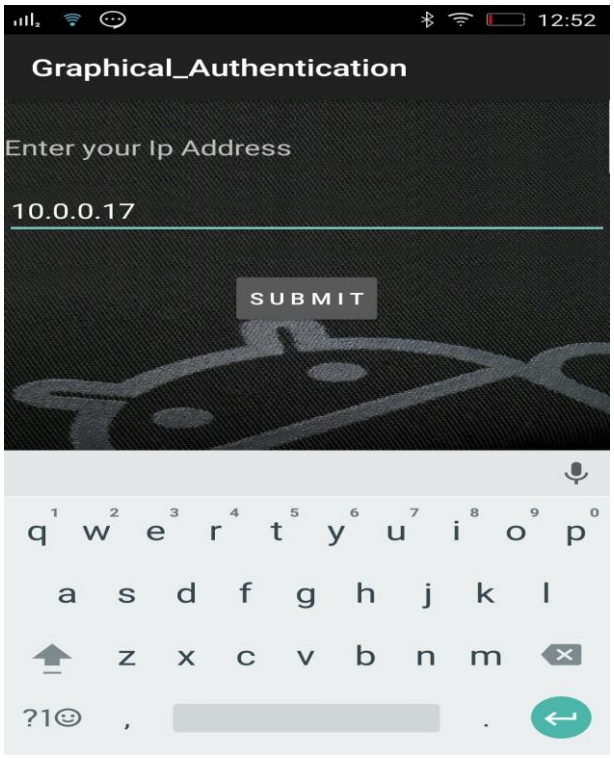
The banking services we provide are called virtual money concept, initially the user credited with rupees and if user is in need to transfer the money to some other account the user go to his withdrawal and enter the amount to transfer. The voucher id generated for the amount you entered. You can share the voucher id to the particular user. He moves to the deposit link and enter the voucher id given by you. The amount will be DEBITED from your account and CREDITED to depositor account.

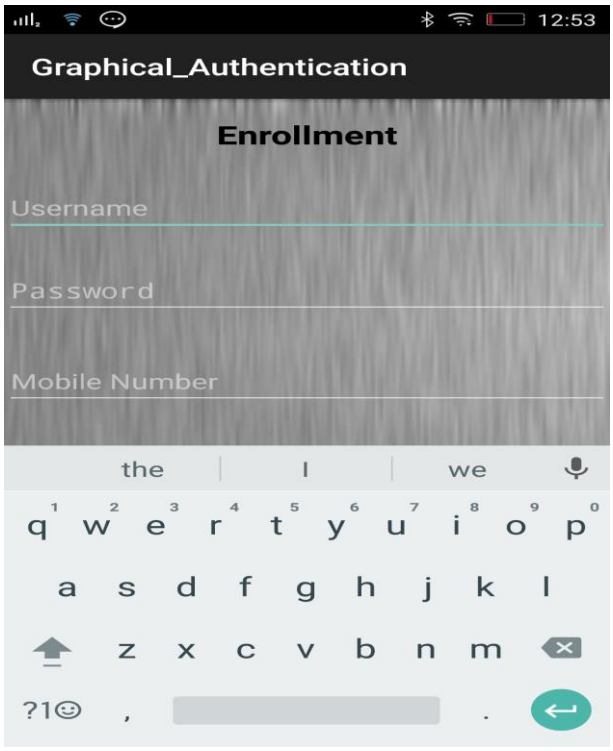
System Features

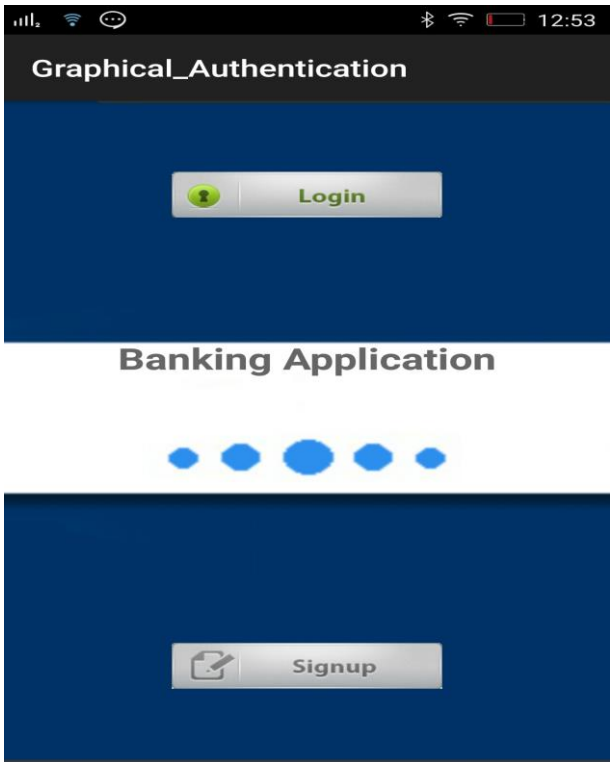
- Qrcode for Application download.
- GUI is handled to some extent.
- Ant build.
- Recycling of Keystore files.
- Micro-App storage for ease of access.
- Security enforcement for keystore and apk files.

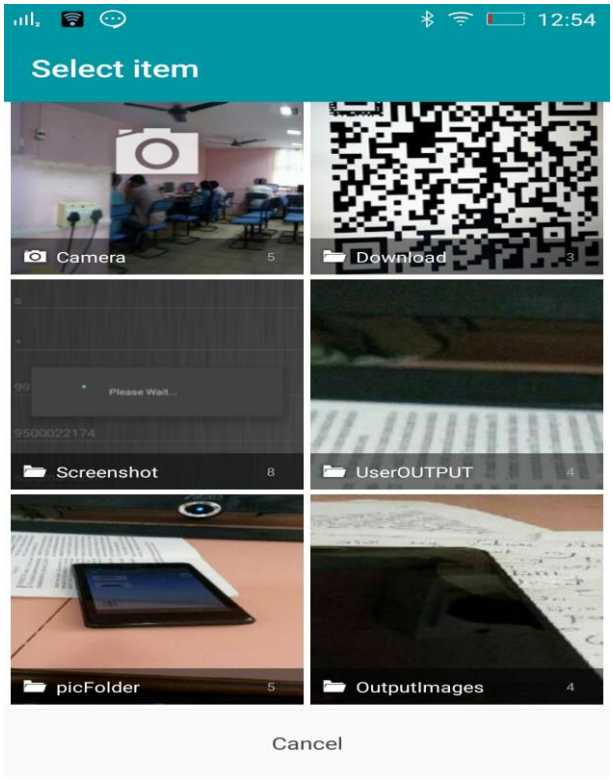
5. Implementation and Results

Screenshots:

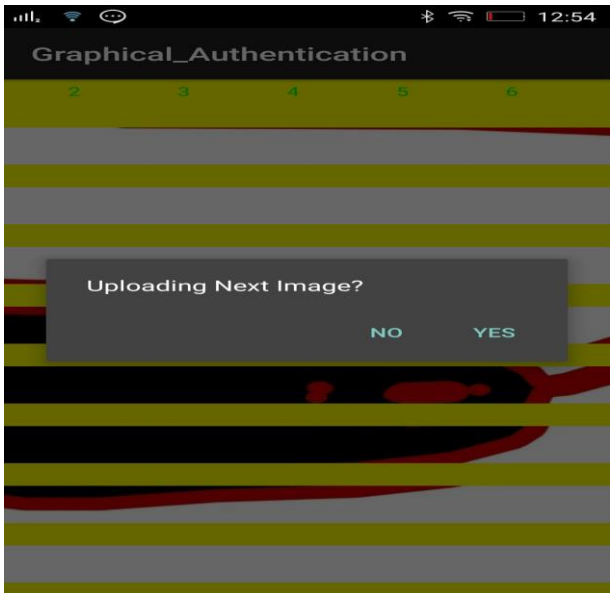

12:52
Graphical_Authentication
Enter your Ip Address
10.0.0.17
SUBMIT

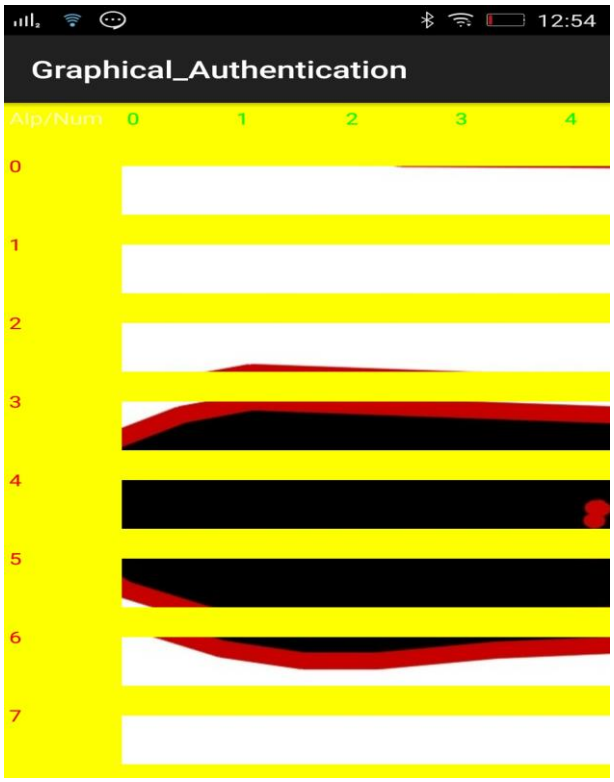

12:53
Graphical_Authentication
Enrollment
Username
Password
Mobile Number


12:53
Graphical_Authentication
Login
Banking Application
Signup

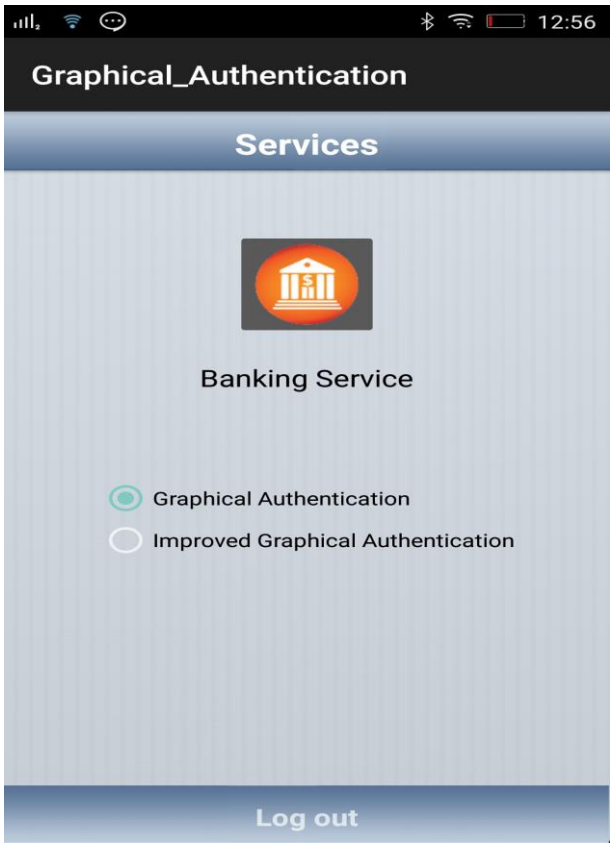

12:54
Select item
Camera
Download
Screenshot
UserOUTPUT
picFolder
OutputImages
Cancel

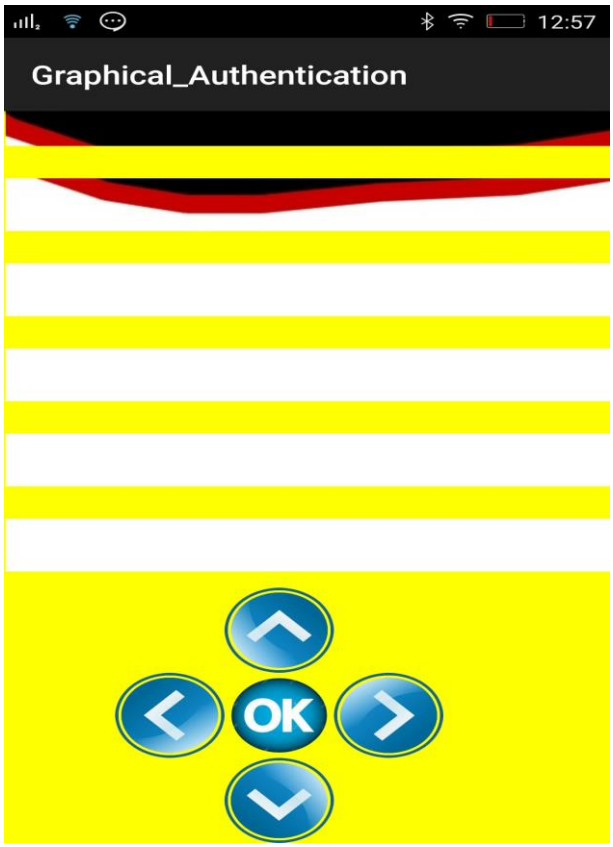

12:54
Graphical_Authentication

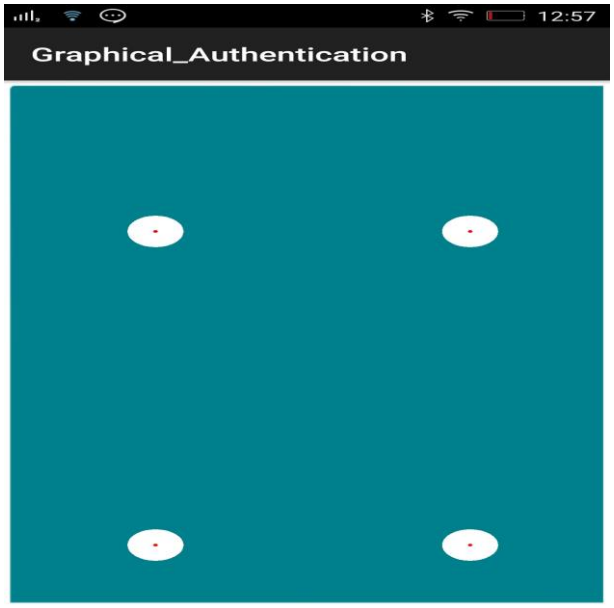

12:54
Graphical_Authentication
2 3 4 5 6
Uploading Next Image?
NO YES

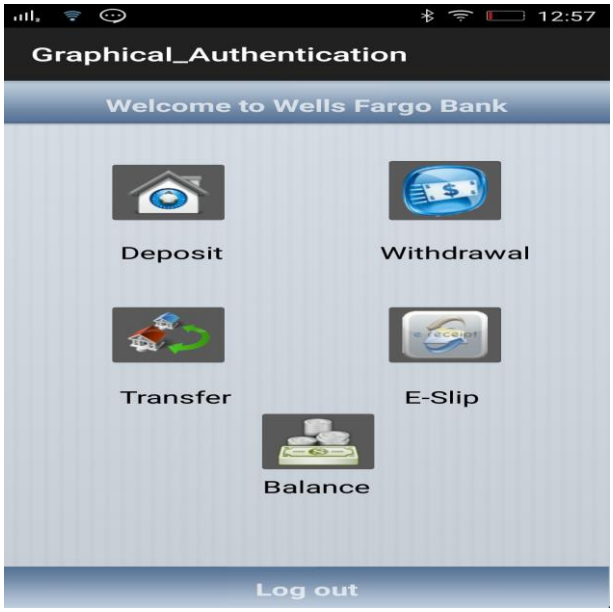

12:54
Graphical_Authentication
Alp/Num 0 1 2 3 4
0
1
2
3
4
5
6
7

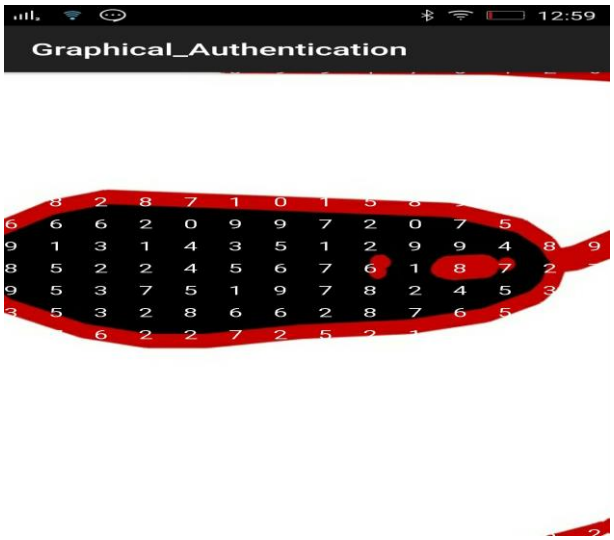

12:55
Graphical_Authentication
Banking Application
Username
Password
Home
Submit
FORGOT PASSWORD

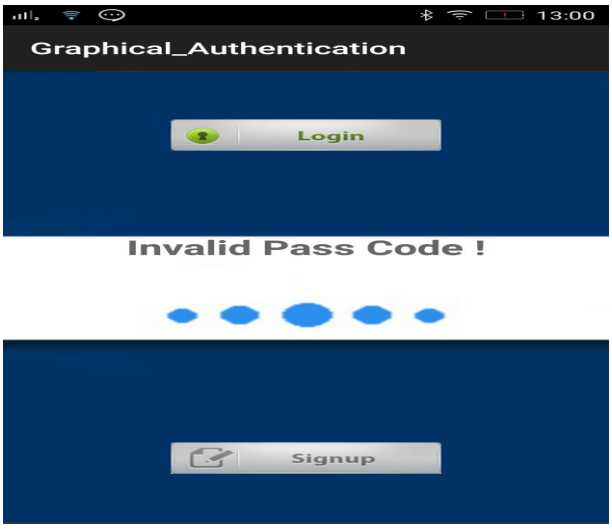

12:56
Graphical_Authentication
Services
Banking Service
Graphical Authentication
Improved Graphical Authentication
Log out

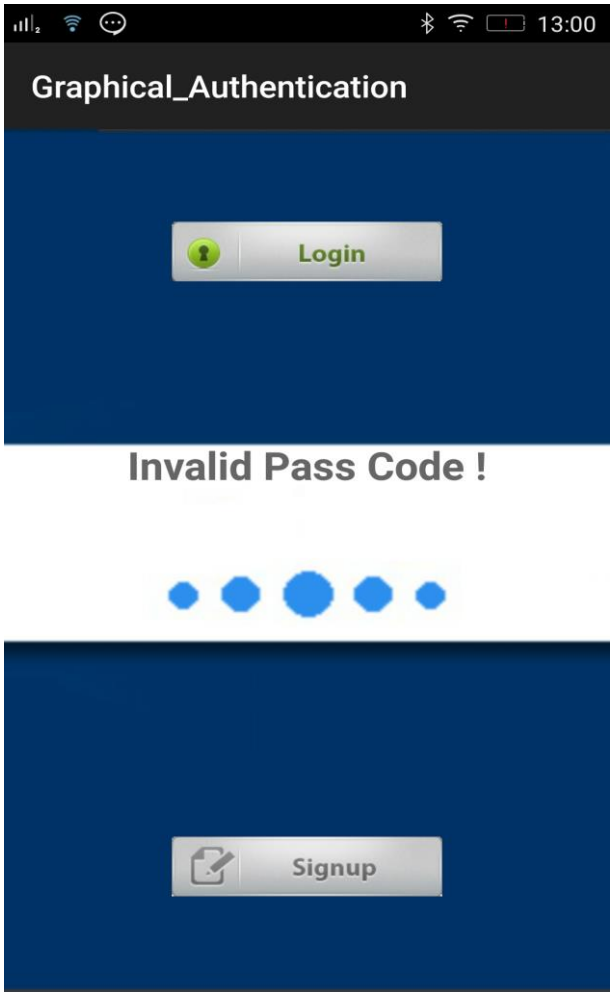

12:57
Graphical_Authentication
OK


12:57
Graphical_Authentication


12:57
Graphical_Authentication
Welcome to Wells Fargo Bank
Deposit
Withdrawal
Transfer
E-Slip
Balance
Log out







6. Conclusion

Authentication using Graphical images will provide higher resistance than the existing approach. Advantages is with ease and usefulness of the idea.

References

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[4] Rupavathy N, Dr Carmel Mary Belinda and Alex David S, "Traffic obstruction handling with image processing" International Journal of Civil Engineering and Technology 8(10), pp 56-62.

[5] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[6] "Realuser," http://www.realuser.com/.

[7] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "Thedesign and analysis of graphical passwords," in Proceedings of the8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[8] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[9] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[10] Rupavathy N, Dr Carmel Mary Belinda and Nivedhitha.G, "A mobile application using IoT enabled navigation system for bus riders" International Journal of Engineering &Technology, Vol 7 (1.7) (2018) 71-74.

[11] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[12] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords? a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.