# Graphical Base Authentication

**Nayan Namdeorao Yerakade**
M. Tech Student
Department of Computer Science and Engineering
Vathsalya Institute of Science and Technology Hyderabad

*Abstract*— In secured graphical authentication system, we are going to focus on security at the time of authentication and security of the database. The security of the database is important because of the user credentials. In this project we have to develop registration page and login page. Previously the work has been done for the android system, and now we have to develop it for the web application. "The web application is for providing cloud storage space".

***Key words:*** Graphical Password, Authentication, Password Image, Security, Protection Encryption

## I. INTRODUCTION

The aim of the proposed system is to provide the user with the more secure authentication based on condition. In this project, the proposed system is an Advanced Authentication System for providing more security to highly confidential data. Normally, authentication is based on the biometric thumb, Finger detection, palm detection or Eris scan. They are considered as the most secure for authentication but this system is providing Graphical password system based on Knowledge based system. In the unusual condition there is a high chance where authorities may be forced to give access. Here, Advanced Authentication System is adaptive and can be properly used for data security purpose. The proposed system is using graphical password for normal authentication but in threat it is using gesture detection. Because of increasing threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Users interact with security technologies either passively or actively. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction. Today there is an increasing recognition that security issues are also fundamentally human computer interaction issues.

Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise privacy concerns and smart card usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time. Yet traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit. The "password problem," as formulated by Birget, arises because passwords are expected to comply with two conflicting requirements, namely:

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be accounts of the same user; they should not be written down or stored in plain text. Meeting these conflicting requirements is almost impossible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure way. Many problems that users have with alphanumeric passwords are related to memorability of secure passwords. In an attempt to create more memorable passwords, graphical password systems have been devised. In these systems authentication is based on clicking on images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented. In recent work we have created a new kind of graphical password system, called Pass Points, and have done studies of its human factors images used in the password system. Changed frequently, and should be different on different characteristics compared to alphanumeric password [33,34]. In this paper we report on further research on usability and memo ability of our system under different conditions. In specific we investigate the effect of the tolerance, or the margin of error, allowed when entering one's password points and the effect of the choice of image used in password system.

## II. RELATED WORK

Every plan should be linked with some objectives. The planning helps us in concentrating their efforts on the most important jobs rather than wasting time on the lesser important work. The purpose of planning is also to minimize the cost of performance and eliminate unproductive efforts. It also helps the management in adopting and adjusting according to the changes that take place in the environment. Planning also provides a basis for teamwork as when the goals are properly defined assignments can be fixed and all the members can start contributing in the achievement of these objectives. Planning gives a sense of direction and ensured that efforts are being put to useful purpose instead of being wasted. Planning also facilitate control because without planning there will be nothing to control.

### *A. Modules*

#### *1) Image Discretization module*

In this module the image has to be divided into the grid as per the selection of the user. i.e. no. of rows and columns is decided by the user.

 

*2) Login Indicator Generator*

It generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for user during the authentication phase. One principle is to keep the indicators secrete from the people other than the user.

*3) Horizontal and Vertical Axis Control Module*

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag and scroll functions for users to control both bars. Users can scroll either bar using the arrows provided to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. Both the bars are circulative.

*4) Communication Module*

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe fro m being eavesdropped and intercepted.

*5) Password Verification Module*

This module verifies the user password during the authentication phase. Pass square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

*6) Upload/Download Module*

As the authentication system is implemented as an authentication for the web application which provides the storage space to the user as the cloud service. The user is going to have his/her personal space over the cloud in which one can upload or download his/her files.

*7) Database*

The database server contains several tables that stores user accounts, passwords (ID numbers of pass images and the positions of pass squares), and the time duration each user spent on both registration phase and login phase. Using FHE the contents in the database is encrypted, and to efficiently check the equality the FHE scheme done the equality check without decryption.

## III. SYSTEM DEVELOPMENT

At this stage, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set..

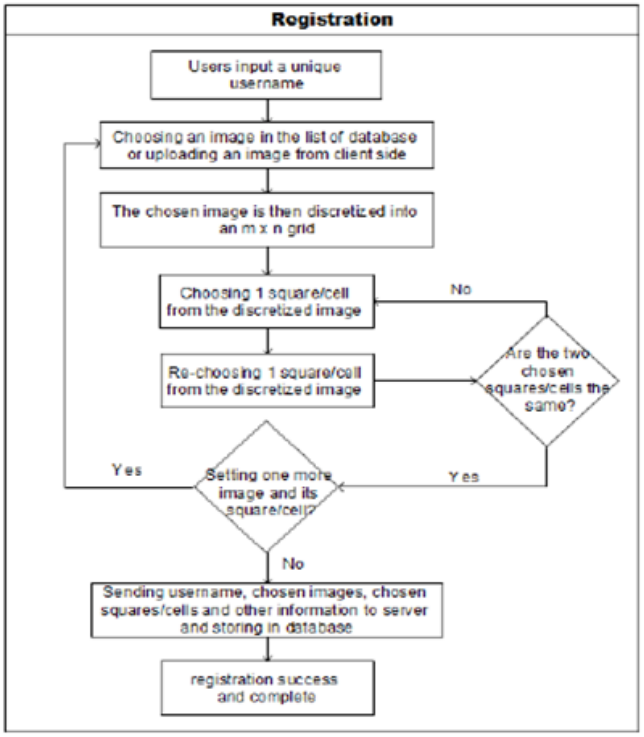


Fig. 1: The flowchart of registration phase in PassMatrix

### *A. Authentication Phasea*

Figure is the flowchart of the authentication phase. At this stage, the user uses his/her username, password and login indicators to log into PassMatrix. The following describes All the steps in detail:

1) The user inputs his/her username which was created in the registration phase.
2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can also be delivered through a predefined image or by audio feedback that we have mentioned in the previous section.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is and the pass-square is in the grid of the image.
4) Repeat step 2 and step 3 for each pre-selected passimage.
5) The communication module gets user account information from the server through HttpRequest POST method.
6) Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix

 

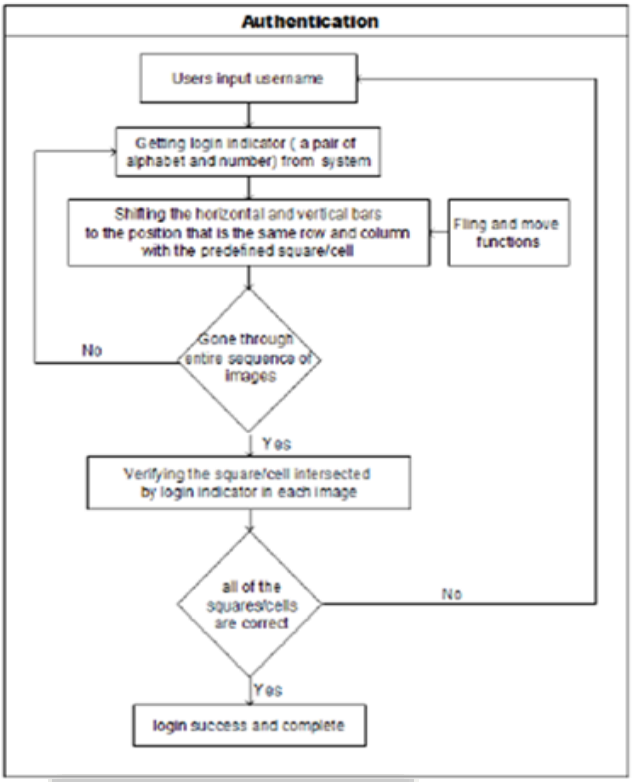


Fig. 2: The flowchart of authentication phase in PassMatrix

## ACKNOWLEDGEMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members specially my father who is always supportive of me.

## REFERENCES

[1] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.

[2] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "Pas: predicate-based authentication services against powerful passive adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[3] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on, vol. 3. IEEE, 2009, pp. 90–95.

[4] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760–767.

[5] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.

[6] "Black hat: Google glass can steal your passcodes,"https://www.technologyreview.com/s/529896/black-hatgoogle- glass-can-steal-your-passcodes/.

[7] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[8] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phonelock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI'11. New York, NY, USA: ACM, 2011, pp. 197–200.

[9] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.

 