International Journal of Engineering & Technology, 7 (2.14) (2018) 97-100

International Journal of Engineering & Technology

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

Research Paper

User Authentication Using Grid Based Method

Siti Noratiqah Md Ariffin, Mohd Fadzil Abdul Kadir*, Ahmad Nazari Mohd Rose, Mohamad Afendee Mohamed, Abd Rasid Mamat

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Tembila Campus, 22200 Besut, Terengganu, Malaysia.
**Corresponding author E-mail: fadzil@unisza.edu.my*

Abstract

Grid recognition authentication is a method of securing user logins. This project is based on user authentication in Smartphone using grid, images, and pattern. It is an innovation from the existing security lock that used in the Smartphone. A smartphone usually consists the authentication techniques such as draw a pattern or inserting a password. But nowadays, those techniques are not completely secure because it is very easy to break through different type of attack like brute force, dictionary attack or key logger. In this project, a tool based Grid Based Method will be developed which is important to increase the security of the smartphone that using an iOS platform. By using this tool, the codes are difficult to break because the grids are hidden behind the image. Users can identify the cells that were selected in a grid during the registration stage.

Keywords: *User authentication; Grid based method; iOS, tool.*

1. Introduction

Preventing data and information from being accessed by unauthorized users are highly important for some organization or user. The confidentiality of data must be secured from the attackers to avoid the data from being stolen. User authentication is one of the important security measures that used to protect the confidentiality of the data. User authentication can be defined as a process of authenticating or certifying user identity to access to the certain information or application. Without verification, the data are vulnerable to the unauthorized person or users that can easily corrupt the information for malicious purpose [1].

Traditionally, alphanumeric passwords are widely used for user authentication but this method is known to have some problem with the security (susceptible to many attacks). This method is easy to implement due to users are commonly choose a short or an easy password, which are easy to remember. Users tend to write down their password on the paper or any device to make it easy to remember [2].

As for the alternative, this project focuses on user authentication using graphical password as the innovation to solve the problem. Graphical password was designated by Blonder. This method is easier because image is easy to remember or recognize rather than memorizing a number or text password. This project will be implementing in the iOS platform.

Grid Based Approach (GBA) is a technique used to complete this project. GBA is a method used to secure user logins by selecting cells in a grid that represented the authentication. User is then authenticated by the server based on the cells selected.

This paper is organized by dividing into sections. Section 2 for the related works involving existing techniques. Section 3 discussed the method used in this project. Section 4 proposed the development of the project. Section 5 presents the result for this project. Section 6 concludes the outcomes of this project.

2. Related Work

This section will be focused on analyzing the information gathered from literature review about this project. In this section also will highlight the differences between the existing graphical passwords techniques and approaches, which being adapted into authentication application environment.

Authentication is a process of validating user identity by verifying user-provided evidence [3]. It is a critical area of security research and practice. To manage user authentication, there are several techniques that can be practice such as:

Token based authentication-For example: key cards, bank cards, smart cards.

Biometric based authentication-For example: Fingerprints, iris scan, facial recognition.

Knowledge based authentication-For example: Alphanumeric password, graphical password

Passwords are the most broadly used authentication method. Passwords can be divided into two categories, which are alphanumeric and graphical passwords.

Graphical password schemes were introduced by Blonder in 1996 [4]. The password is set by allowing the arrangement to display the tap region to a user and requires user to position these tap regions in a location and sequence within the graphical image, which the user desires the password to be set at.

PassPoints is another Blonder's idea of representing the password by multiple click on an image [1]. Around areas of the image within which the user clicks, there are no artificial predefined boundaries meaning that user may choose any region as the click points in the image. After the sequence of the click points is choose, the system cryptographically encrypts the password and calculated a tolerance region around the chosen pixels. In login process, to make a valid click the user will have to click within this tolerance.

The others techniques that are used for authentication are biometric. Déjà vu algorithm was proposed by Dhamija and Perrig in year 2000. Based on a hash virtualization technique, users are required to select a number of pictures from image gallery [5]. Instead of selecting several positions on the image, Déjà vu displayed several random images that should be selected by the users as their password. The enhancement done by Blonder's scheme is the size of images are much larger than the size of the correct position should be selected.

Passfaces the commercial product of Real User Corporation is an algorithm, which require a user to choose a face from a grid of faces image [5]. This technique requires user to select the previously seen human face picture from a grid of nine faces, which one of the face is the known face and the rest is the decoy faces.

DAS algorithm requires users to draw a pattern precisely without getting any hint. The pattern must be draw in the same manner as been done during the registration phase [6]. Users have to draw their password on a 2D grid. The password is composed of the grid cells that the user passes through while drawing [7].

3. Methodology

Some grid based approaches are perfectly designed for authentication. GBA ensure users to select cells based on a grid for authentication. This approach is mostly having similar methods of authentication as for example DAS which proposed by Jermyn et al., where users need to draw the passwords on a 2D grid. The coordinate of the password is stored in order. During the authentication process, users need to redraw the picture and the user will be authenticated if the drawing is matched the grid in the same order.

GBA practices a little bit different style with other method which every time for login or authentication process, the server generates an interface with a grid on it. User will enter a password based on the grid. As GBA is defined on image, every pixel of area selections plays important roles. Figure 1 shows the example of Grid Based method.

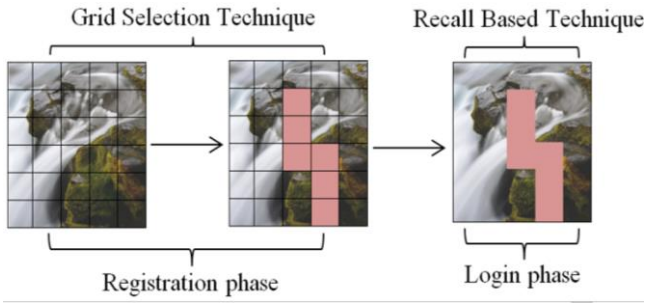

Fig. 1: Grid based method

4. Development

In this section, it involves the development of the authentication system. Grid based method and recall based technique will be applied in this authentication system. The development process can be represented through framework and flowchart.

Based on the framework shown in Figure 2, there are two modules which differentiate each of the process. In password initialization module require user to setting up the password. User will be given an option to choose an image from the application database to be used as the background image password. From the selected image, users need to select any cells and the number of the selected cell will be stored in a database for authentication purpose use in the next module.

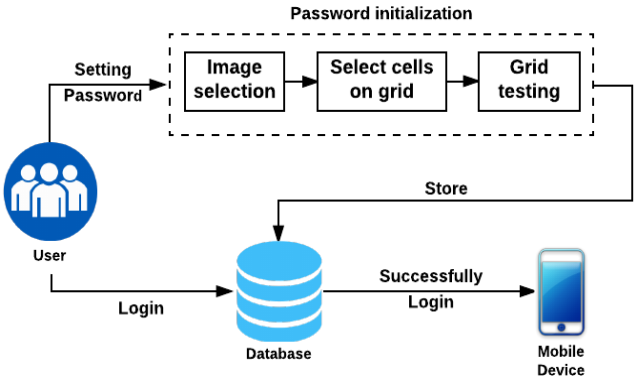

Fig. 2: Framework

The authentication module is start up upon the application is open. User will be asked to click on the cells as a means of entering a password. The number of the cell will be compared to the initial value stored in the database. If the value is same, user will be authenticated and the application will grant permission to access data in the device.

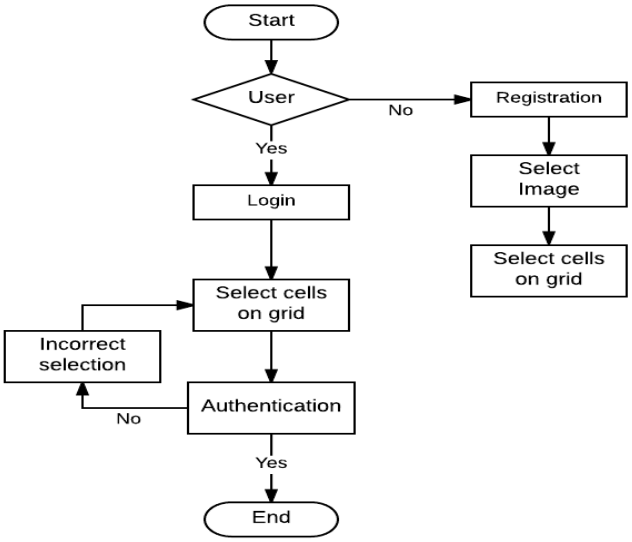

Fig. 3: Flowchart

Figure 3 shows the flowchart of the authentication system. When users open the application, the new users are require to register. During the registration phase, users need to choose image from the gallery. Once the image was selected, next phase is selecting cells in the grid. Users have to select any cells in the grid to complete the process. All the data will be saved into the database. If the users have already registered, he/she are available to proceed to the login phase. During the login process, users need to select the same cells as selected during the registration phase. The application will compare the data with the data that stored during the registration phase. If the compared data are correct, then the user authentication process is successful.

5. Results and discussion

In this section, the result of the implementation is presented. This tool was implemented in a diary application to ensure that the data kept in the diary are protected. The application consists of four section which are main section, registration section, login section and diary section.

Figure 4 shows the main section consist of two buttons which are register button for the new user and diary button for the registered user. User may choose either these two buttons to proceed to the next step.

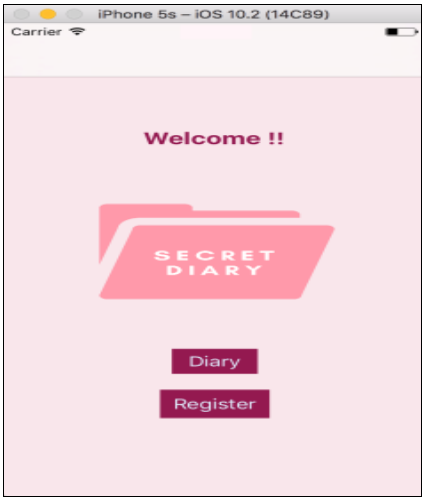

Fig. 4: Main page

For the registration section, users have to choose an image from their smartphone gallery as shown in Figure 5. Then, Figure 6 shows that users need to select cells on the grid.

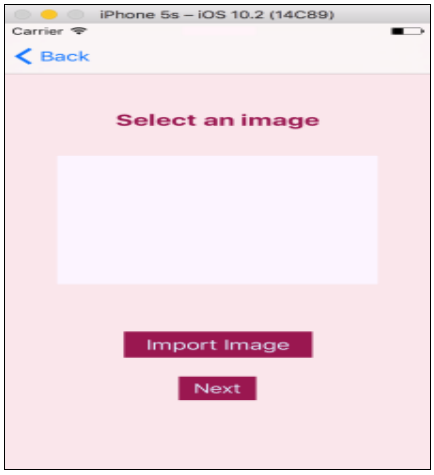

Fig. 5: Image selection

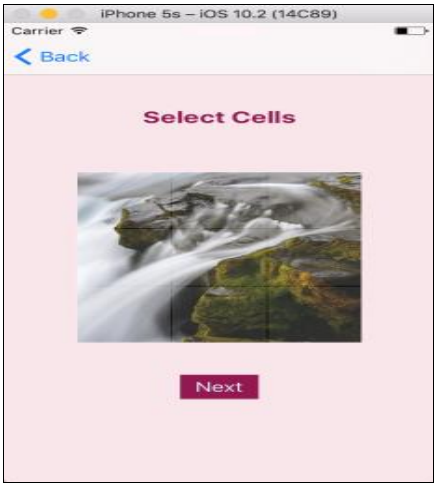

Fig. 6: Grid selection (registration phase)

Figure 7 shows the login section. This section requires users to select the cells on the image based on the cells selection during the registration phase. This section is connected to the database where are the data are stored from registration phase.

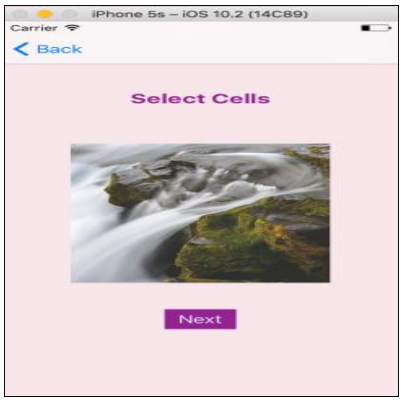

Fig. 7: Grid selection (login phase)

When users select the correct cells, the authentication process is success. After being authenticated, users are directly connected to their diary as shown in Figure 8. The authentication process is completed.

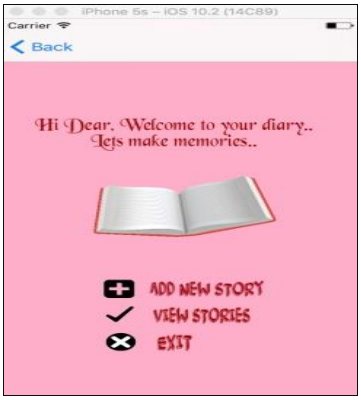

Fig. 8: Diary main page

If users select exit button, they will able to logout and perform other activity. If they want to log in to the diary, they have to pass the grid selection phase during the login session.

6. Conclusion

This project helps to solve conflicts of hard to remember password and creating easily attack password. By using GBA as an approach, most of attackers' problem such as brute-force attack, dictionary and shoulder surfing attack can be solved.

In this paper, we develop an implementation of pattern-based password authentication scheme for minimizing shoulder surfing attack. With the combination of two techniques, we can prove that this method is secure. The grid selection technique during the user registration process requires users to select the grids as their chosen password. Users can choose any patterns or styles as there is no limit for the user to select how many grid they like for their password. Lastly, recall based technique during the user login process significantly increase the grid password space.

References

[1] Biswas SS & Sankar S (2014), Comparative study of graphical user authentication approaches. *International Journal of Computer Science and Mobile Computing* 3, 361–375

[2] Agarwal G, Singh S & Shukla RS (2010), Security analysis of graphical passwords over the alphanumeric passwords. *International Journal of Pure and Applied Sciences and Technology* 1, 60–66.

[3] Havighurst R (2007), Chapter 1: User identification and authentication concepts. In D. Todorov (Ed.), *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Florida: CRC Press, pp. 1–64.

[4] Vinothini T, Rajesh I & Kirupa Rani D (2014), Multiple grid based graphical text password authentication. *International Journal of Research in Engineering and Technology* 3, 502–507.
[5] Ugochukwu EE & Jusoh YY (2013), A review on the graphical user authentication algorithm: Recognition-based and recall-based. *Journal of Information Processing and Management* 4, 238–252.
[6] Bhanushali A, Mange B, Vyas H, Bhanushali H & Bhogle P (2015), Comparison of graphical password authentication techniques. *International Journal of Computer Applications* 116, 11–14.
[7] Dunphy P & Yan J (2007), Do background images improve draw a secret graphical passwords? *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 36–47.