Proceeding of ICITS 2020 e-ISSN: 2716-6732
6th International Conference on Information Technology & Society
November 11th, 2020, Selangor, MALAYSIA

Mobile Image Authentication System

Sharmila Mat Yusof and Nur Aliyah Mohd Roszaini

School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, Sintok, Kedah, Malaysia.

ysharmila@uum.edu.my, *nuraliyahhh123@gmail.com*

Abstract. Nowadays, mobile users are spending lots of time communicating, browsing the Internet, performing online banking, purchasing etc. As such, the mobile devices are storing countless amount of confidential data such as personal email inboxes, bank accounts, social media accounts and other sensitive information. Thus, it is vital to protect data on the smartphones. The traditional protection is by using a textual password as a common part of the authentication process. Using this traditional authentication system in protecting users' data would lead to a compromised data security. The use of easily guessed password would lead to an easy attempt to break it whereas if the password is hard to guess, then it is often difficult to memorize. To address this problem, this project proposes a new approach of mobile authentication system, which is the graphical scheme of authentication based on images. The mobile application consists of the series of images that form an authentication system. The application is very useful for users who requires authentication application for their mobile devices. The design and development of the application follows the Rapid Application Development (RAD) methodology. The content analysis method is used to gather the requirements of the application. The prototype of Mobile Image Authentication (MIA) was developed based on the requirements that have been gathered. A usability evaluation has been conducted to evaluate the usefulness of the prototype. The result of the evaluation shows that MIA application is useful, easy to use and secure. Overall, the respondents are satisfied with the functions performed by the MIA application.

Keywords: image authentication, mobile application, recognition based, recall based.

INTRODUCTION

Mobile images authentication system is an alternative solution to a text-based authentication system motivated particularly by the fact that humans can remember images better than text (Kirkpatrick, 1894; Paivio et al., 1968). This graphical authentication system can make passwords more memorable and easier to use by users and at the same time more secure and usable (Marom et al., 2009). In addition, this type of authentication scheme can also benefit the disabled people who can easily do authentication by just clicking on images rather than typing the alphanumeric strings.

Recently, many networks, computer systems and Internet-based environment are trying to use the graphical authentication schemes for their users. However, most of the existing graphical authentication schemes were vulnerable to shoulder-surfing. An example of such a system is Draw-a-Secret (DAS) introduced by Jermyn et al. (1999) which is a recall based graphical password scheme with a grid in which user draws his password using a mouse or stylus. The user's drawing is considered as his password and the password's space is depend on the size and the complexity of the grid. As the grid size become larger, it will increase the password's space and the complexity of the grid. In addition to the shoulder-surfing threat, this system is prone to human error due to grid complexity as the grid size increases. This is because the users have difficulty in guessing the middle points when they have a very large grid size.

Thus, this project intent to create an easy to use and less complex authentication system based on images to secure users' data on their mobile devices. In addition, the mobile application is also expected to benefit the disabled people in authenticating themselves by using a less complex and useful authentication technique. This project proposes one of the main categories of graphical user authentication that are broadly used nowadays which is recognition-based authentication technique (image selection and click-based).

BACKGROUND AND RELATED STUDIES

There are various graphical password techniques that have been developed nowadays. The first graphical password introduced was in 1996 by Blonder (Gokhale & Waghmare, 2013). There are three main categories of authentication which are recognition-based, recall-based and hybrid-based authentication system (Baby Maruthi & Sandhya Rani, 2017). This section elaborates few techniques that have been developed based on the graphical password authentication system.

Recognition Based Technique

For recognition-based technique, users are required to select some images from a set of random images presented during registration stage. Then, during authentication stage users will be authenticated based on the correct sequence of images selected during registration. Some of the works are presented as follows:

Dhamija & Perrig (2000) propose a technique where users are required to select images during registration, and they need to recognize those pre-selected images in the correct sequence during authentication.

Jensen (2004) present a technique where user need to select images based on theme in a sequence to form a password. The theme images are displayed for selection in thumbnail in a 5 x 6 grid. Then the same process user needs to recognize the images in a correct sequence to be successfully authenticated. For this technique, the number of images is limited to 30 which make the size of password space small. For each image, a number is allocated where a selection sequence during authentication process will generate a numerical password. The numerical password may be shorter than the textual password. Thus, to solve the problem, user may select two images at a time on a single click to increase the password space size. However, this option will increase the complexity and difficulty for the authentication process.

Mihajlov et al. (2011) propose technique that also let user to select images as password in a grid of 30 images during registration. During authentication, real and decoy images are presented to users in a grid of 4 x 3. The image position will change at every login. User needs to select the real images with a correct sequence to be successfully authenticated. The approach is not strongly tolerant of shoulder surfing due to the small size of grid and the password images are fixed.

Recall Based Technique

In recall-based technique, user must recall or reproduced something that have been chosen or selected during registration stage. The recall-based technique can be categorised into pure recall-based and cued recall-based techniques. The difference between the two techniques is that the later provides clue during the authentication process. Some of the works are presented as follows:

Blonder (1996) proposes a cued recall-based technique where user is presented the fixed image with predetermined tap regions during registration. User needs to click the tap regions in a specific sequence to set up as his password. During authentication, user need to click at the estimated areas of those pre-set tap regions in a correct sequence. The advantage of this technique is that the image serves as a clue to user to easily recall his password. Thus, this technique is more convenient compared to the textual password. However, the drawback of this technique is its memorable password space.

Syukri et al. (1998) propose a pure recall-based signature technique where user need to draw his password using mouse during registration. The exact password needs to be reproduced during authentication process. This approach does not require user to memorise the signature and it is hard to be faked. However, the weaknesses of this approach are its difficulty to draw signature using mouse and to reproduce the same signature during authentication. The use of pen input device can overcome this problem, but it can be expensive.

Jermyn et al. (1999) propose a pure recall-based technique where user must draw an image on a two-dimensional grid where each cell is denoted by x and y axis. The values of touch grids are stored in the order of drawing. Then during authentication user must redraw the similar image touching the same coordinates of the grid. This technique has a better password space compared to the textual password. The weakness of this technique is user might forget their stroke order. In addition, user sometimes choose a weak password that is exposed to threat such as graphical dictionary and replay attack.

Varenhost (2004) presents a technique of pure recall-based where user need to scribble any design or text as his password (Passdoodle) during registration stage. The advantage of this technique is user can easily remember his password but sometimes he tends to forget the order of the scribble that he has created. The technique however vulnerable to shoulder surfing, spyware and guessing.

Wiedenbeck et al. (2005) propose a cued recall-based technique that can overcome the limitation of the Blonder technique. In this technique, user can click on any place on the image during registration process and there is no pre-set click points like in Blonder technique. When the user clicks on the image, tolerance value surrounding the clicked point will be calculated. During authentication process, user can click on any tolerance area of the image in a correct sequence. The technique solves the Blonder's technique limitation but still the users can have more difficulty to learn his password compared to textual passwords. In addition, the login time is more than textual password.

Hybrid Based Technique

In hybrid-based technique, the registration and authentication stages combine both recognition-based and recall-based steps before user is authorized to access the system/devices. The main works for this technique are presented as follows:

Haque & Imam (2014) propose a new hybrid graphical password authentication system that combines both recognitions based and recall based techniques. The technique consists of two stages of registration and authentication/login while authentication is done in two steps (recall and recognition). In registration stage, user needs to enter personal details, choose images and questions. To set the answer for the question, user need to set the Region-Of-Answer (ROA) for the selected images. During authentication process, user need to enter the correct username and sequence of images for the first step. In second step user need to click at the correct ROA of the image to answer the question. After the successful entry of both steps then only user is authorized to have access to a particular system/device.

Gokhale & Waghmare (2016) propose an improved and modified version proposed by Haque and Imam (2014). The technique is similar which consists of the two stages of registration and authentication with the addition of few functions to make the system more secure. Among the added functions are the generation of the secret pass and session password after the selection of images. In this technique, the selected images are displayed in panel to increase the recall of the images later.In the authentication phase user need to click on three ROA instead of one. The system also add the new function of forget password.

The above hybrid approach (Haque & Imam, 2014; Gokhale & Waghmare, 2016) are highly secure especially againts shoulder surfing but the password space is very large, quite complex and the authentication process requires extra time.

All the above techniques have been reviewed and analysed in terms of its security and usability metrics. It is found that some techniques are strongly secure but not easy to use. On the other hand, some techniques are user friendly but not strong in security. In addition, some of the techniques are not strongly secure and cannot resist brutal force attack or shoulder surfing. Thus, the project attempts to propose and implement a technique that is easy to use as well as resistant to shoulder surfing.

METHODOLOGY

The methodology used for this project is adopted from the RAD (Rapid Application Development) approach. The approach is an agile project management strategy for software development (Lucidchart, 2018). The RAD approach is targeting at developing software in a short span of time, which is suited for this project as it needs to be completed within few months. This approach offers greater efficiency, faster development, and effective communication (Beynon-Davies et al., 1999).

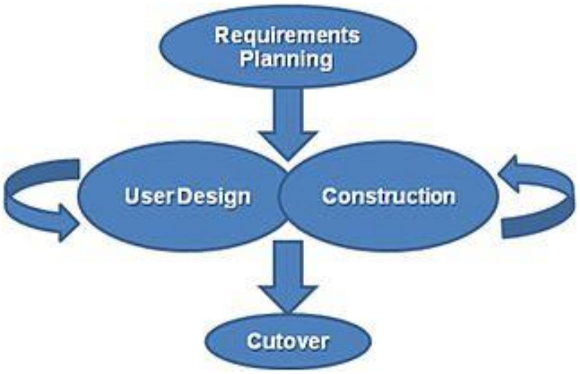


FIGURE 1. The phases of the RAD approach

Figure 1 illustrate the stages involved in the methodology. The requirement-planning phase is used to gather all the requirements of the MIA application. The technique used in this phase is content analysis where the document reviews and application reviews were performed to gather the main functions of the mobile application. Based on the reviews done, the requirements were modelled and documented using Unified Modelling Language (UML) diagrams such as use case, sequence, and class diagrams. Then, the user design and construction phases were performed together where the user interface and functions of MIA application were developed. Finally, in a cutover phase, we implement the application and conduct a usability evaluation to get the respondent’s feedback of MIA application.

THE DESIGN AND DEVELOPMENT OF THE MIA APPLICATION

This section outlines the design and development of MIA application that follows the first three phases in RAD approach. This section is divided into two parts: (1) the requirements of MIA application and (2) the development of the prototype. A requirement gathering process was carried out by using a method of analyzing related documents and applications from the Internet. Most of the documents and applications were searched using search engine by keywords such as “mobile image authentication system”, “authentication system”, “locking application” and “image password”. The related documents and applications found were used to obtain the requirements of the MIA application. Table 1 lists the requirements gathered from the requirements gathering process.

TABLE 1. List of the Requirements of the MIA application

No.	Requirement ID	Requirement Description
	MIA_01	**Create User Account**
1.	MIA_01_01	User must setup his or her account for the application.
2.	MIA_01_02	User needs to fill in the form that consists of username, email, and password.
3.	MIA_01_03	User must select images to create his or her own graphical password in a sequence. Each password consists of 3 images.
	MIA_02	**Authenticate User**
1.	MIA_02_01	User must choose the correct graphical password (the registered images) with a correct sequence to be successfully authenticated.
2.	MIA_02_02	User would be blocked if they have entered invalid username or graphical password more than 3 times attempt.
3.	MIA_02_03	If the user is blocked, the application will ask the user’s email to reset his or her new graphical password.

The requirements presented in Table 1 were translated into the application functionality. The next process is visualizing and modelling the requirements of the application using the appropriate modelling method and tools. To visualize and model the requirement, the Unified Modelling Language (UML) was used. The three behavioral diagrams namely use case, sequence and class diagram were constructed to show the structural components of the application. The diagrams were drawn using Star UML. Figure 2,3 and 4 illustrates the related diagrams.

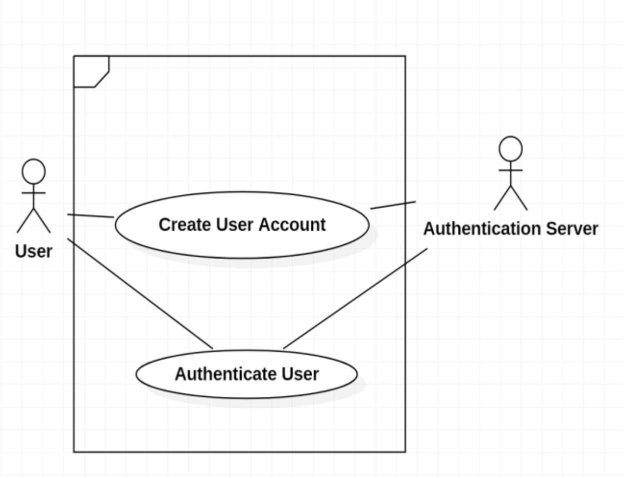


FIGURE 2. The use case diagram of MIA application

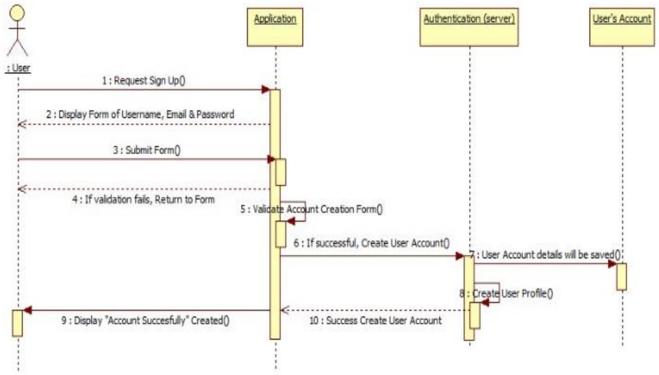

: User
Application
Authentication (server)
User's Account
1 : Request Sign Up()
2 : Display Form of Username, Email & Password
3 : Submit Form()
4 : If validation fails, Return to Form
5 : Validate Account Creation Form()
6 : If successful, Create User Account()
7 : User Account details will be saved()
8 : Create User Profile()
9 : Display "Account Succesfully" Created()
10 : Success Create User Account

FIGURE. 3. The sequence diagram of Create User Account

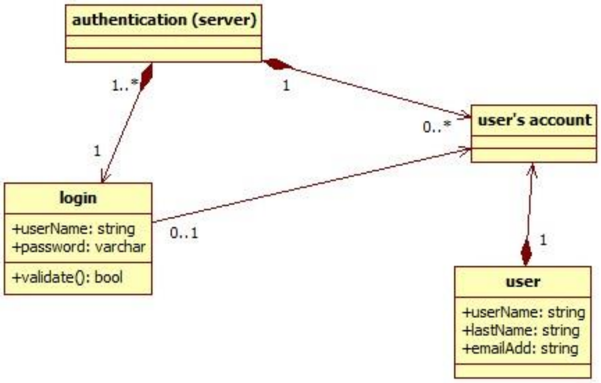
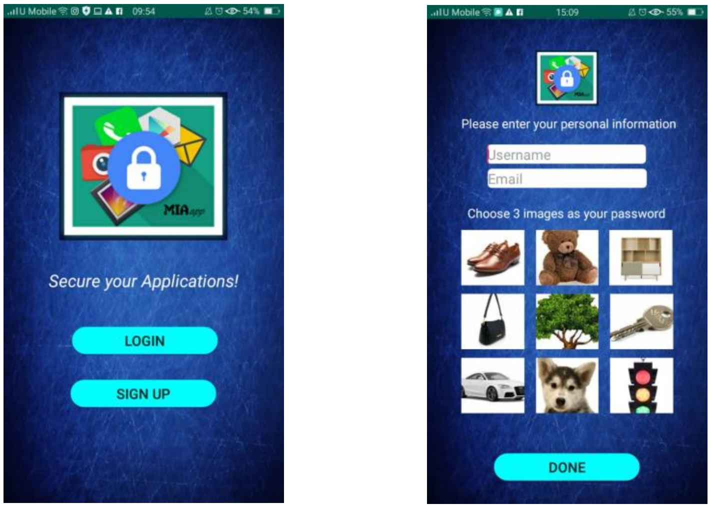


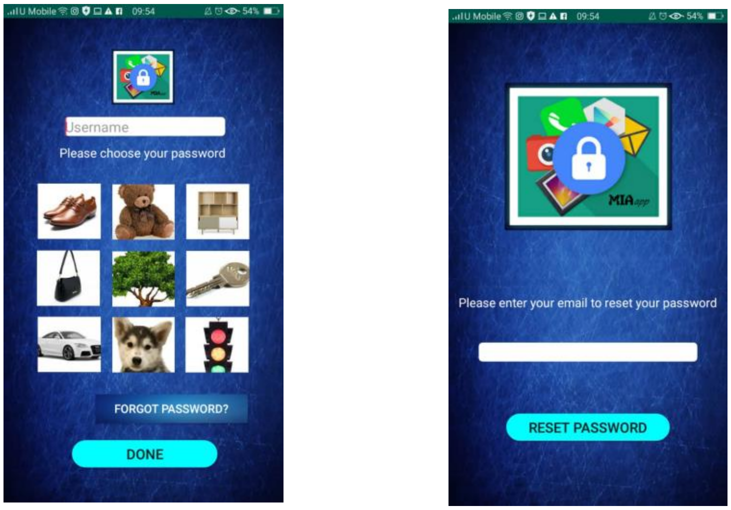
FIGURE 4. The class diagram of the MIA application

A prototype of MIA application was developed using Android Studio. The database used is MySQL which run on XAMPP server. The screenshots in Figures 5 and 6 show the selected interfaces of MIA application.


MIA app
Secure your Applications!
LOGIN
SIGN UP
Please enter your personal information
Username
Email
Choose 3 images as your password
DONE

(a) (b)

FIGURE 5. The main interface (a) and the sign-up interface (b).


Username
Please choose your password
FORGOT PASSWORD?
DONE
MIA app
Please enter your email to reset your password
RESET PASSWORD

(a) (b)

FIGURE 6. The login interface (a) and the reset password interface (b).

THE EVALUATION OF THE MIA APPLICATION

The Evaluation Setting

A usability evaluation was conducted using 30 respondents of students from different background of courses in Universiti Utara Malaysia (UUM). The respondents participated in the evaluation are on a voluntary basis and were randomly approached in School of Computing and Inasis MAS. The instruments used for the usability evaluation were the MIA application and a post-task questionnaire. The post task questionnaire consists of 33 items in two sections. In section A, the respondents were asked on their demographic questions. Section B asked the respondents on any improvement to be made or problems with MIA application. In addition, the respondents were also asked on their opinions on the usability of MIA application based on the Likert scale represented by one (1) for strongly disagree, two (2) for disagree, three (3) for neutral, four (4) for agree and five (5) for strongly agree. The respondents were asked to perform the following tasks in completing the evaluation: (1) read and signed a consent form, (2) performed the functions of MIA application as stated in the experiment procedure and (3) answer the post-task questionnaire.

The Respondents' Demographic Information

Based on the analysis of the respondents' demographic information, 7% of them were male while 93% of them were female. Based on the college information of the respondents, 6% of them were from College of Law, Government and International Studies (COLGIS), 27% of them were from College of Business (COB) and 67% of them were from College of Art and Science (CAS). Most of the respondents, which is 65% of them, use pin number, 29% of them use pattern and 6% of them use image as their passwords to lock their mobile devices. Additionally, 73% of the respondents have heard about the image password, 4% of them were not sure while 23% of them never heard about the image password. It was found that 62% of the respondents never use any application of password based on images, 3% of them were not sure and 35% of them have already used the application of password based on images.

The Usability of the MIA Application

An analysis was conducted to get the respondents' opinions on the usability of MIA application in Section B of this post-task questionnaires. The section measures the respondents' experiences when interacting and performing the task given. It also measures on how well the users can learn and use the application based on the usefulness, ease of use, security, and overall satisfaction of the application. Tables 2, 3, 4, 5 and 6 reported the analysis and average of the respondents' responses. The respondents rated four or five of the post-task scales for the four aspects of the usability evaluation. Only a few rated one, two and three.

TABLE 2. The respondents' responses on the satisfaction of the usability evaluation

The post-task questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Average
Overall, I am satisfied with the ease of completing this task	0 (0.00)	0 (0.00)	2(6.66)	13 (43.33)	15 (50.00)	4.43
Overall, I am satisfied with the amount of time it took to complete this task	0 (0.00)	0 (0.00)	1(3.33)	12 (40.00)	17 (56.66)	4.53

TABLE 3. The respondents' responses on the usefulness of MIA application

The post-task questionnaire items	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**	**Average**
MIA App enhances my effectiveness on securing information or data.	0 (0.00)	0 (0.00)	3 (10.00)	17 (56.66)	10 (33.33)	4.23
MIA App enables me to accomplish tasks more quickly.	0 (0.00)	0 (0.00)	3 (10.00)	17 (56.66)	10 (33.33)	4.23
MIA App saves my time when I use it.	0 (0.00)	0 (0.00)	3 (10.00)	14 (46.66)	13 (43.33)	4.33
MIA App meets my needs.	0 (0.00)	0 (0.00)	6 (20.00)	13 (43.33)	11 (36.66)	4.17
MIA App does everything I would expect it to do.	0 (0.00)	1 (3.33)	5 (16.66)	18 (60.00)	6 (20.00)	3.97
MIA App is useful in overall.	0 (0.00)	0 (0.00)	2 (6.66)	11 (36.66)	17 (56.66)	4.50

TABLE 4. The respondents' responses on the ease of use of MIA application

The post-task questionnaire items	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**	**Average**
MIA App is easy to use.	0 (0.00)	0 (0.00)	1 (3.33)	11 (36.66)	18 (33.33)	4.57
MIA App is user friendly.	0 (0.00)	0 (0.00)	2 (6.66)	11 (36.66)	17 (56.66)	4.50
MIA App is flexible.	0 (0.00)	0 (0.00)	1 (3.33)	14 (46.66)	15 (50.00)	4.47
MIA App requires fewer steps to accomplish what I want to do.	0 (0.00)	0 (0.00)	5 (16.66)	13 (43.33)	12 (40.00)	4.23
MIA App is easy to learn how to use it.	0 (0.00)	0 (0.00)	4 (13.33)	8 (26.66)	18 (33.33)	4.47
I can use MIA App without written instructions.	0 (0.00)	0 (0.00)	5 (16.66)	19 (63.33)	6 (20.00)	4.03
I can easily remember how to use it.	0 (0.00)	0 (0.00)	7 (23.33)	9 (30.00)	14 (46.66)	4.23
I do not notice any inconsistencies as I use MIA App.	1 (3.33)	0 (0.00)	7 (23.33)	14 (46.66)	8 (26.66)	3.93
I can recover from mistakes quickly and easily when using MIA App.	0 (0.00)	0 (0.00)	8 (26.66)	12 (40.00)	10 (33.33)	4.07
I can use MIA App successfully every time.	0 (0.00)	0 (0.00)	9 (30.00)	8 (26.66)	13 (43.33)	4.13

TABLE 5. The respondents' responses on the satisfaction of MIA application

The post-task questionnaire items	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**	**Average**
I am satisfied with MIA App.	0 (0.00)	0 (0.00)	2 (6.66)	12 (36.66)	16 (53.33)	4.47
I would recommend MIA App to my friend.	0 (0.00)	0 (0.00)	0 (0.00)	14 (46.66)	16 (53.33)	4.53
MIA App works the way I want it to work.	0 (0.00)	0 (0.00)	2 (6.66)	14 (46.66)	14 (46.66)	4.4
I feel I need to have MIA App.	0 (0.00)	0 (0.00)	3 (10.00)	10 (33.33)	17 (56.66)	4.47
MIA App is wonderful and pleasant to use.	0 (0.00)	0 (0.00)	1 (3.33)	15 (50.00)	14 (46.66)	4.43

TABLE 6. The respondents' responses on the security of MIA application

The post-task questionnaire items	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**	**Average**
MIA App only kept a single credential.	0 (0.00)	0 (0.00)	3 (10.00)	18 (60.00)	9 (30.00)	4.20
MIA App authenticates users.	0 (0.00)	0 (0.00)	1 (3.33)	19 (63.33)	10 (33.33)	4.30

MIA App is secure and makes my life easier.	0 (0.00)	0 (0.00)	0 (0.00)	22 (73.33)	8 (26.66)	4.27
I prefer to use MIA App.	0 (0.00)	0 (0.00)	1 (3.33)	14 (46.66)	15 (50.00)	4.47

The result from the evaluation shows that MIA application were received well by the respondents. The respondents said they were satisfied with the features and functions in the MIA application. The analysis from the respondents' feedbacks also stated the specific functions of the MIA application which are registration, authentication and reset password were useful and not complicated. They described the MIA application is essential to lock their applications or mobile devices and stated that they are considering using this application.

CONCLUSION AND FUTURE WORKS

The proposed MIA application is using the recognition-based technique because it is easy to use and secure compared to the traditional text-based authentication system. Overall, the MIA application is a strong authentication system that are against shoulder surfing and can be used for highly secure system. In future, a foreseen function that can be added to improve security is to add secret questions and answers to authenticate users when they want to reset the password. This will make the application more secure but still easy to access.

REFERENCES

1. Baby Maruthi, P. & Sandhya Rani, K. (2017). Recall Based Authentication System-An Overview. *International Conference on Innovative Applications in Engineering and Information Technology*, 3(1), 121-125.
2. Beynon-Davies, P., Carne, C., Mackay, H. (1999). Rapid application development (RAD): an empirical review. *Eur J Inf Syst*, 8**,** 211–223. https://doi.org/10.1057/palgrave.ejis.3000325
3. Blonder G. E. (1996). Graphical passwords. United States Patent 5559961.
4. Dhamija, R. & Perrig, A. (2000). Deja Vu: A User Study Using Images for Authentication. *Proceedings of 9 USENIX Security Symposiums*.
5. Gokhale, A & Waghmare, V. (2013). Graphical Password Authentication Techniques: A Review. *International Journal of Science and Research,4* (7), 279-285.
6. Gokhale, A & Waghmare, V. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *Procedia Computer Science, 79*, 490-498. https://doi.org/10.1016/j.procs.2016.03.063.5(http://www.sciencedirect.com/science/article/pii/S1877050916001940)
7. Haque, Md & Imam, Babbar. (2014). New Graphical Password: Combination of Recall & Recognition Based Approach. 8. 320-324. 10.5281/zenodo.1091324.
8. Jansen, W. A. (2004). Authenticating Mobile Device Users Through Image Selection. *Data Security*.

9. Jermyn, A., Mayer, A., Monrose, F., Reiter, M. K. & Rubin, a. (1999). The design and analysis of graphical passwords. Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.
10. Kirkpatrick, E. A. (1894). An experimental study of memory. *Psychological Review*, *1*(6), 602–609. https://doi.org/10.1037/h0068244
11. Lucidchart, "Lucidchart," Lucid Software Inc, 23 May 2018. [Online]. Available: https://www.lucidchart.com/blog/rapid-application-development-methodology. [Accessed 22 May 2019].
12. Marom, M., Towhidi, F. & Habibi Lashkari, A. (2009). Pure and cued recall-based graphical user authentication. 2009 International Conference on Application of Information and Communication Technologies, AICT 2009. 1-6. 10.1109/ICAICT.2009.5372534.
13. Mihajlov, M., Borka, M. & Ilievski, M. (2011). ImagePass – Designing graphical authentication for Security. Proceedings of the 2011 7th International Conference on Next Generation Web Services Practices, NWeSP 2011.10.1109/NWeSP.2011.6088188.
14. Paivio, A., Rogers, T. & Smythe, P. C. (1968). Why are pictures easier to recall than words?. *Psychonomic Science*, 11(4),137-138.
15. Syukri, A. F., Okamoto, E. & Mambo, M. (1998). A User Identification System Using Signature Written with Mouse. Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science. (1438), 403-441.
16. Varenhorst, C. (2004). Passdoodles; a Lightweight Authentication Method. Massachusetts Institute of Technology, Research Science Institute.
17. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Nasir Memon. (2005). Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1-2), 102-127.