# GRAPHICAL PASSWORD AUTHENTICATION IMPLEMENTED IN WEB- BASED SYSTEM

# ABSTRACT

Authentication is the method of giving persons access to system object based on user’s uniqueness. If the code match, the process will be accomplished and user will get the approval to access the system. Text-based password scheme follows the guidelines such as at least 8 characters long, should combine upper case and lower-case and digits. User have problem to remember their complicated password over time due to the limitation of human brain, user tend to forget about their password. User tend to use the same password for all type of account. So, if one account is hacked, the possibility for other account to be hack is high. Other than that, choosing the simple textual-based password may increase its vulnerability for attacks or intrusions. Hence, graphical password authentication by using passpoints scheme has been introduced in this project. Graphical password authentication by using passpoints scheme is a model to identify the most likely regions for user to click in order to create graphical password. The operation of the purposed scheme is simple and easy to learn for user since they familiar with textual graphical password scheme. In conclusion, this graphical password scheme will make it easier for user to do their authentication process since it is easy to remember and hard to guess by others.

# TABLE OF CONTENT

**CONTENTS PAGE**

[DECLARATION ii](#_bookmark0)

[CONFIRMATION iii](#_bookmark1)

[ACKNOWLEDGEMENT iv](#_bookmark2)

[ABSTRACT vi](#_bookmark3)

[TABLE OF CONTENT vii](#_bookmark4)

[LIST OF FIGURES 1](#_bookmark5)

[LIST OF TABLES 2](#_bookmark6)

[LIST OF ABBREVIATIONS/TERMS/SYMBOLS 3](#_bookmark7)

[LIST OF APPENDICES 4](#_bookmark8)

[CHAPTER 1 5](#_bookmark9)

[INTRODUCTION 5](#_bookmark10)

* 1. [Background 5](#_bookmark11)
  2. [Problem Statement 6](#_bookmark12)
  3. [Objectives 6](#_bookmark13)
  4. [Project Scope 7](#_bookmark14)
  5. [Limitation of work 7](#_bookmark15)
  6. [Thesis Structure 8](#_bookmark16)

[CHAPTER 2 10](#_bookmark17)

[LITERATURE REVIEW 10](#_bookmark18)

[2.1 Introduction 10](#_bookmark19)

[2.2. PassPoint Method 11](#_bookmark20)

* 1. [Blonder Graphical Password Scheme 12](#_bookmark21)
  2. [Security in Graphical Password Authentication 12](#_bookmark22)
  3. [Multiple-image schemes 14](#_bookmark23)
  4. [Déjà Vu 15](#_bookmark24)
  5. [Summary 16](#_bookmark25)

[CHAPTER 3 17](#_bookmark26)

[METHODOLOGY 17](#_bookmark27)

* 1. [Introduction 17](#_bookmark28)
  2. [System Design 17](#_bookmark29)
     1. [Framework 17](#_bookmark30)
     2. [Flowchart 18](#_bookmark31)
     3. [Use Case Diagram 21](#_bookmark32)
     4. [Sequence Diagram 23](#_bookmark33)

[3.4 Summary 25](#_bookmark34)

[CHAPTER 4 26](#_bookmark35)

[IMPLEMENTATION 26](#_bookmark36)

* 1. [Introduction 26](#_bookmark37)
  2. [User Interface of the System 26](#_bookmark38)
     1. [Registration Phase 27](#_bookmark39)
     2. [Login Phase 32](#_bookmark40)

[CHAPTER 5 RESULT AND ANALYSIS 38](#_bookmark41)

* 1. [Introduction 38](#_bookmark42)
  2. [User Register 38](#_bookmark43)
  3. [User Login 39](#_bookmark44)

[CHAPTER 6 CONCLUSION 41](#_bookmark45)

* 1. [Introduction 41](#_bookmark46)
  2. [System Contribution 41](#_bookmark47)
  3. [Future Work 41](#_bookmark48)

[REFERENCES 43](#_bookmark49)

[APPENDIX 45](#_bookmark50)

# LIST OF FIGURES

Figure 2.1 A Sample of PassPoint Method 11

Figure 2.2 Graphical Password Scheme Suggested by Blonder 12

Figure 2.3 Passfaces™ Method… 14

Figure 2.4 Déjà vu Method 15

Figure 3.1 Framework 18

Figure 3.2 Flowchart 19

Figure 3.3 Use Case Diagram for New User 21

Figure 3.4 Use Case Diagram for Existing User 21

Figure 3.5 Sequence Diagram for Registration Phase 23

Figure 3.6 Sequence Diagram for Login Phase 24

Figure 4.1 Home Interface for Graphical Password System 27

Figure 4.2 Registration Page 28

Figure 4.3 Registration Password 28

Figure 4.4 User's First Click 29

Figure 4.5 User's Second Click 29

Figure 4.6 User's Third Click 30

Figure 4.7 User's Fourth Click 30

Figure 4.8 User's Fifth Click 31

Figure 4.9 Successful Registration Interface 31

Figure 4.10 Login Interface 33

Figure 4.11 Login Password 33

Figure 4.12 First Click in Login Phase 34

Figure 4.13 Second Click in Login Phase 34

Figure 4.14 Third Click in Login Phase 35

Figure 4.15 Fourth Click in Login Phase 35

Figure 4.16 Fifth Click in Login Phase 36

Figure 4.17 Success Login Interface 36

Figure 4.18 Failed Login Interface 36

# LIST OF TABLES

Table 5.1 Test case for register 39

Table 5.2 Test case for login 40

# LIST OF ABBREVIATIONS/TERMS/SYMBOLS

GPA Graphical Password Authentication LR Literature Review

# LIST OF APPENDICES

|  |  |  |
| --- | --- | --- |
| APPENDIX | TITLE | PAGE |
| A | Gantt Chart FYP I | 46 |
| B | Gantt Chart FYP II | 47 |

# CHAPTER 1

# INTRODUCTION

* 1. Background

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most of the authentication system nowadays uses an integration of username and password [2]. The problem with the password is that it requires user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate number, parent name, phone number sometimes their own name which are very much predictable or complex passwords which they overlook so they might be use the same password for different accounts or they jot down their password somewhere. Moreover, user is vulnerable to various attacks. Text-based passwords faces from security and usability matters.

To overcome these shortcomings of alphanumeric passwords, graphical password schemes have been proposed. In graphical password authentication application by using

passpoints scheme a password contains an image where user can input password with the help of mouse events like click and drag. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by human brain, enhancing the ability to [4]. Strong passwords can be invented which are resistant to guessing, dictionary attack and social engineering.

* 1. Problem Statement

The problem statement that can be describe in this project are user have problem to remember their complicated password over time due to the limitation of human brain, user tend to forget about their password. Next, user tent to use the same password for all type of account. So, if one account is hacked, the possibility for other account to be hack is high. Therefore, choosing the simple textual passwords may increase its vulnerability for attacks or intrusions.

* 1. Objectives

The first objective of the research is

* + 1. To design a Graphical Password Authentication implemented in mobile application.
    2. To implement the Graphical Password Authentication application using PassPoint technique.
    3. To test the effectiveness of Graphical Password Authentication system using PassPoint technique to authenticate user by using web-based system.
  1. Project Scope

The scope for this project is identified which to make the web system process easier. This project concentrates more on the security of the system.

1. Scope of User

* Enter username, password, email during registration and login phase.
* Select an image during registration phase and login phase.
* Click five points during registration phase and login phase.

1. Scope of System

* Sign up – the authentication system let the user select picture and click points in a correct number of clicks.
* Log in – check either the user username, password, image and clicked points are valid and exist in the data store.
  1. Limitation of work

It is a well-known fact that every system has its own limitations including this proposed system. One of the limitations of this application is that it does not have a beautiful and proper interface since the objective of the project is to authenticate user. It only has simple interface with only two spaces for user to insert their username and to input email and to make a selection of picture to use as a password and the submit button.

This project is focusing only on the authentication of a user based on graphical password using passpoints scheme for authentication.

* 1. Thesis Structure

Chapter 1

In this first chapter contain the most important part which is give a basic description on the idea of the whole project. The part of this chapter focuses on the background, problem statement, objectives, project scopes and limitation of work and thesis structure of the project.

Chapter 2

This chapter will describe about the related work of the other researches to gain more understanding of the project idea. The concept of graphical password will be described in this chapter. The existing conventional password and the benefits of the graphical password authentication will be discussed in this chapter from the reading material and sources such as articles, journals, related websites and existing project.

Chapter 3

This chapter will describe about the methodology of this proposed project which is by using passpoints scheme. This chapter will explain more about method and the system requirement about the project.

Chapter 4

This chapter will explain about the implementation of passpoints scheme in graphical password authentication. The implementation shows whereby the system is being developed for the system.

Chapter 5

In chapter 5 show the testing of the system for graphical password authentication and also the result of the successful and failure of user register along with login the system.

Chapter 6

Chapter 6 is the last chapter which conclude the achievement of the expected results, expectations and also future work of this proposed project.

# CHAPTER 2

# LITERATURE REVIEW

2.1 Introduction

This chapter discussed about the related research that is review for Graphical Password Authentication which are being proposed. Generally, this including a few article and journal that related directly and indirectly to the secure graphical password system. All this research was described, summarized, evaluated and clarified. It is a regulation in order to establish the credibility for a better project.

* 1. PassPoint Method

In this paper [1] it is an extended Blonder’s idea by eliminating the predefined boundaries and allowing arbitrary images to be used. The image could be any natural picture or painting then it contains several possible clicks points. As a result, a user can click on any place on an image (as opposed to some pre- dined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence as in Figure 2.1. When using this method user might easily able to quickly create a valid password.

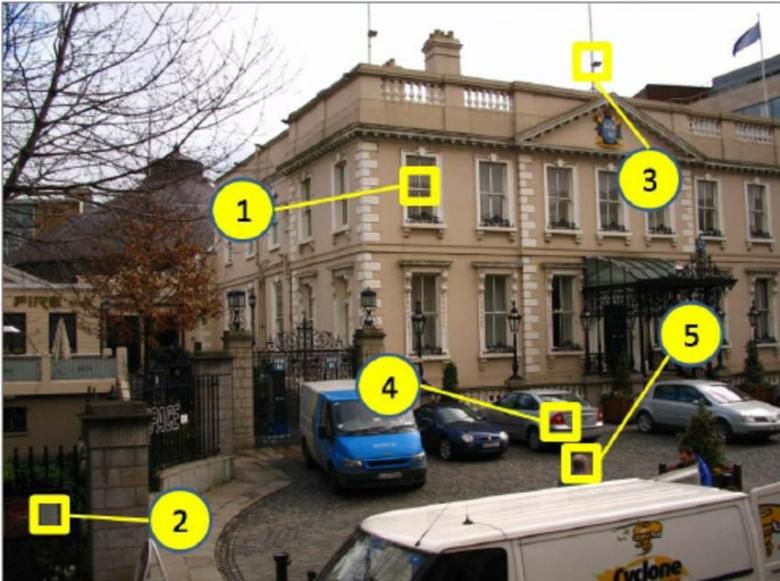


Figure 2.1 A Sample of PassPoint Method

* 1. Blonder Graphical Password Scheme

Single-image based schemes use one single image as a background, and require a user to repeat several actions with an input device, such as clicking or dragging in the same manner as in the registration stage.

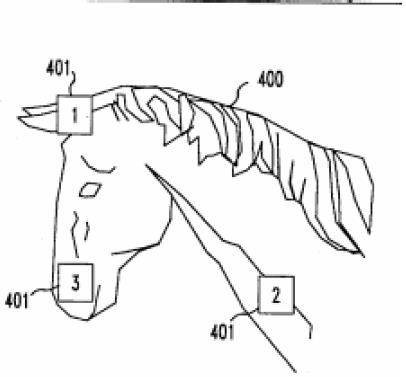


Figure 2.2 Graphical password scheme suggested by Blonder

Blonder [10] gave the initial idea of graphical password. In his scheme, a user is presented with one predetermined image on a visual display and required to select one or more predetermined positions on the displayed image in a particular order to access the restricted resource. The major drawback of this scheme is that user cannot click arbitrarily on the background. The memorable password space was not studied by the author either.

* 1. Security in Graphical Password Authentication

According to the paper [11], the first defence for computer system is authentication. Graphical authentication may offer greater resistance to guessing and capture attacks but there are other attacks against graphical authentication including social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware which those attacks might be threats to the security breach. Authentication mechanism that often being used is the combination of usernames and passwords which is based on textual-based password. Nevertheless, this traditional approach had shown

some disadvantages. The significant consequences of the approach are the user might choose simple password for authentication process or the user can create a strong password however it is hard to be remembered by the user itself.

This paper mentioned about three categories of the graphical authentication scheme which are Drawmetric schemes, Searchmetric schemes and Locimetric system. There are also CAPTCHA, but it is not based on recognition or re-creation password like the other graphical password but it is relied on human (as opposed to computer) abilities to recognize obfuscated text displayed in form of image. There is also hybrid scheme which is made up of combination of two or more schemes.

By using graphical password scheme, it can provide highly secure authentication process by enable the user to remember the complex password easily. And it also can be used as defence to the shoulder surfing, Spybot and similar compromises of user systems. The highly secure authentication system can be achieved by adding some security features in graphical user authentication.

* 1. Multiple-image schemes

In multiple-image schemes, on the other hand, multiple images are presented and a user is required to recognize and identify one or more of it, which are previously seen and selected by the user.

Psychological studies suggest that people are much better at imprecise recall, particularly in recognition of previously experienced stimuli [14]. This class of passwords was shown to be remembered by user for a long period after short perception.

* + 1. Passfaces Method

Passfaces™ is a commercial product by Passfaces Corporation [7], requires a user to select previously seen human face pictures as a password, as shown in Figure

* 1. One problem with Passfaces is that some faces displayed might not be welcomed by certain user. In other words, if a user has to look at some faces, he/she does not like or even dislike., the login process will become unpleasant. Another drawback of Passfaces is that it cannot be used by people who are face-blind (a disease which affects a person’s ability to tell faces apart).



Figure 2.3 Passfaces™ Method

* 1. Déjà Vu

Graphical authentication mechanism based on hash visualization technique is proposed by [5]. In the proposed scheme, the user will have to choose a few pictures from a group of random pictures generated by a program. Then, the user has to identify the selected images during registration before in order to be authenticated. In this research paper, by using graphical authentication the outcome shows that 90% of all the participants success the authentication session while only 70% succeeded using text- based password and PINS. However, this proposed technique uses more time than the traditional approach in terms of average log in time. They also mention the disadvantages of this technique is there are needs to store the details of the images of each user in plaintext in the server. Considering the fact that the password space of textual passwords is much larger than that of Déjà vu is easier to remember.

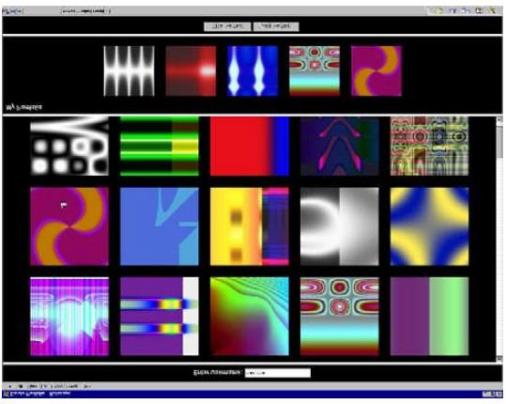


Figure 2.4: Déjà vu Method

* 1. Summary

This chapter is discussed about the literature review that use a reference for development process of this proposed system. The analysis is done to find suitable technique and method for this system.

# CHAPTER 3

# METHODOLOGY

* 1. Introduction

This methodology is the description in the research to achieve the objectives by describing the development of the project. Suitable flow of project can make the system more systematic and effective and performing theoretical analysis of the methods applied to a field of studies.

* 1. System Design

System design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. System design could be seen as the application of system theory to product development.

* + 1. Framework

Framework is a sketch of following process that allows how the system works and happen. Figure 3.1 shows that user can register to the system by enter username, email and phone number and then user is required to select a picture displayed. At this point, user need to click any five points in the picture that had been chosen before. After that, registration information will be saves in database. During login phase, user need to insert the username that has been registered during registration phase. Then, user is required to verify the picture displayed in the application that they had choose during

registration phase. After that, user is required to click five points that they clicked during the registration phase respectively. The system will make a comparison by checking the information with database. The database server will send result whether user have registered or not to the user. Finally, user will be authenticated if the information entered and given by user are all correct.

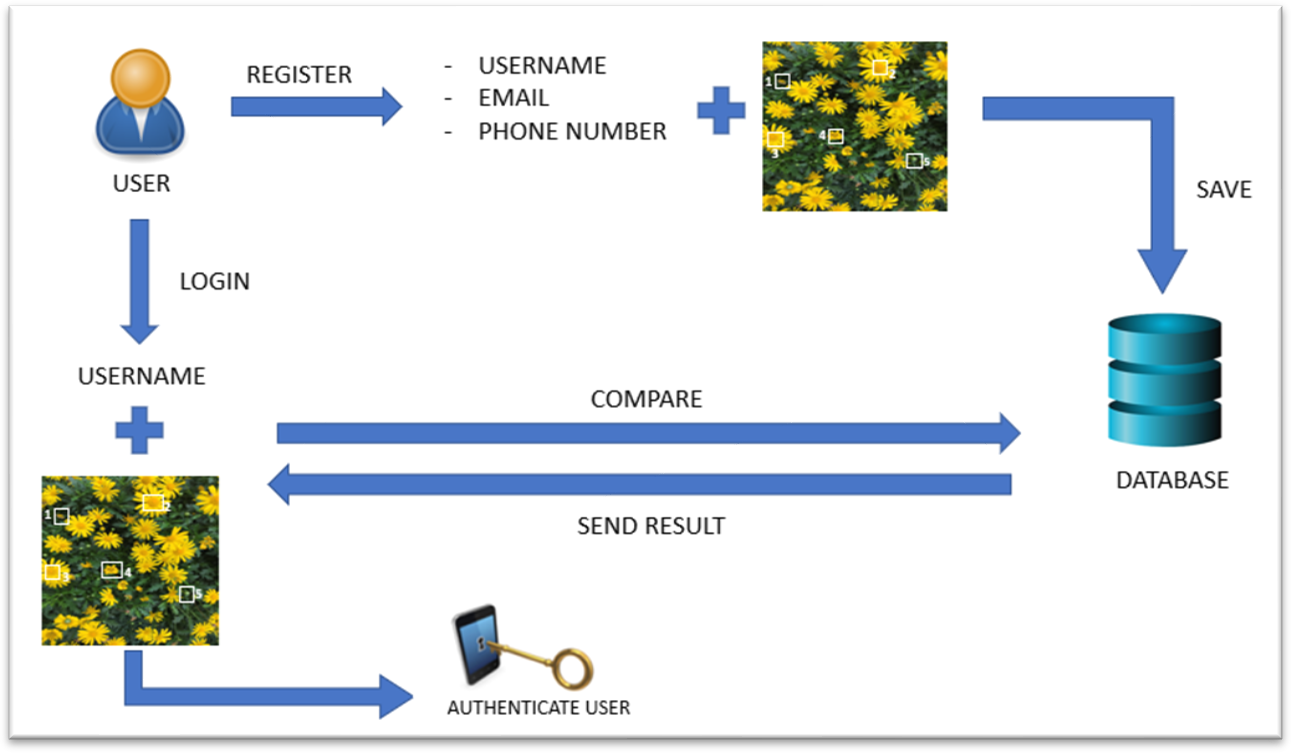


Figure 3.1: Framework of Graphical Password Authentication Using PassPoints Method

* + 1. Flowchart

A flowchart is a diagram that describes a process, system or computer algorithm. In this section, the flowchart for implementing the project will be described. Figure 3.2 shows the flowchart of Graphical Password Authentication by using PassPoint method.

For registration phase, user will enter their name, email and phone number. After that, user is required to select a picture out of 30 images and then they will click five points

within the image. User will legally registered after they had fill all of the requirements needed in the registration phase.

For log in phase, firstly user is required to enter their username that had been registered before. Then, there will be an image that user needed to verify either is it true that is their image or not. If it is, user need to click five spots that they had clicked during registration phase. Lastly, user is authenticated and they can log into the system.

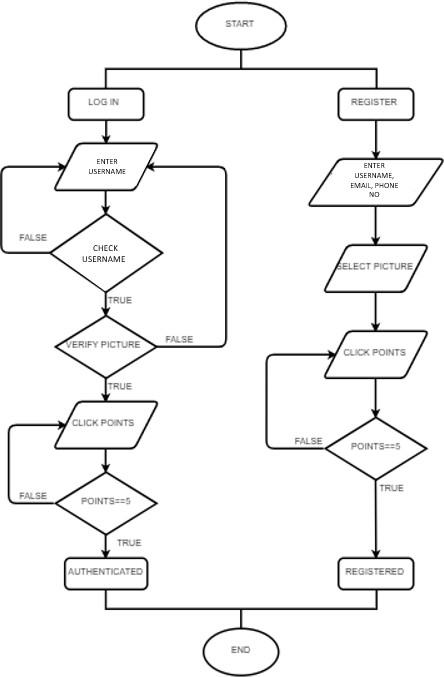


Figure 3.2: Flowchart for Graphical Password Authentication Using PassPoints Method

* + 1. Use Case Diagram

A use case diagram is a graphic representation of the communication among the element in the system [3]. It used in system analysis to identify, clarify, and organize system requirements. The use case is made up of a set of possible orders of interaction between application and user in a particular environment and related to a particular goal. It involves a group of elements for example, classes and interfaces that can be used together in a way that will have an impact greater than the sum of the separate elements combined. The use case should cover all application activities that have consequence to the user.

Figure 3.3 shows the use case diagram for graphical password authentication using Passpoints scheme for new user. By looking at the diagram, four use cases will be found which are create username, create password, select picture and save password. Besides, the actor of this use case diagram is new user. Actor can be defined as something that interact with the system. The actor can be human user or internal and external application. Another important point is to identify the application boundary which are shown in the diagram. The actor user lies outside the system as it is an external user of the application.

Next, figure 3.4 show the use case diagram for graphical password authentication for existing user. There are also four use cases can be found in the diagram which are enter username, enter password, select picture and authenticate.

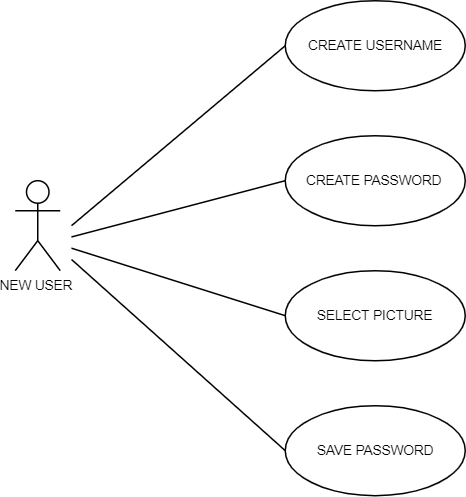


Figure 3.3: Use case diagram for new user

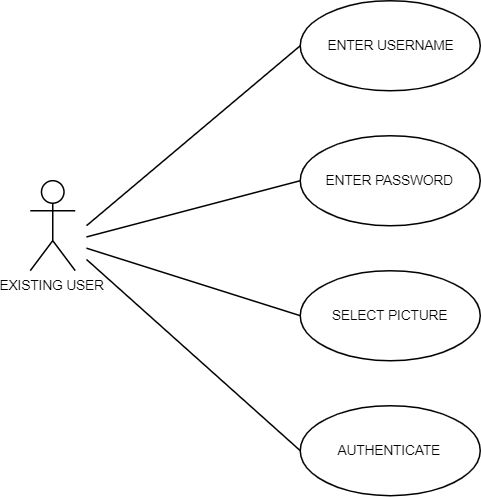


Figure 3.4: Use case diagram for existing user

* + 1. Sequence Diagram

A sequence diagram is an interaction diagram that shows how processes operate with one another and in what kind of order [3]. A sequence diagram also shows object interaction arrange in the sequence. It depicts the object and classes involved in the scenario and the sequence of messages exchange between the object needed to carry out the functionality of the scenario. Sequence diagram are sometime called event diagram or event scenarios.

A sequence diagram shows parallel vertical lines (lifeline), different processes or object that lives simultaneously, the horizontal arrow, the message exchange between them, in the order which they occur in the system. This allow the specification of simple runtime scenarios in graphical manner.

Figure 3.5 will show the sequence diagram of registration process. User need to make the registration by request the registration page from the server. Then, the server will return the registration page. Next, user need to create a username and then, user will be link to page selection of a picture. User need to choose one picture for their password. Next, user will be link to the picture that they choose to click five points in the selected picture. After done with all the clicks, user need to click on “Confirm” button. The server will send and save all value and data that user selects. If the registration process succeeds, the server will response with simple popup message that inform the user the data is saved.

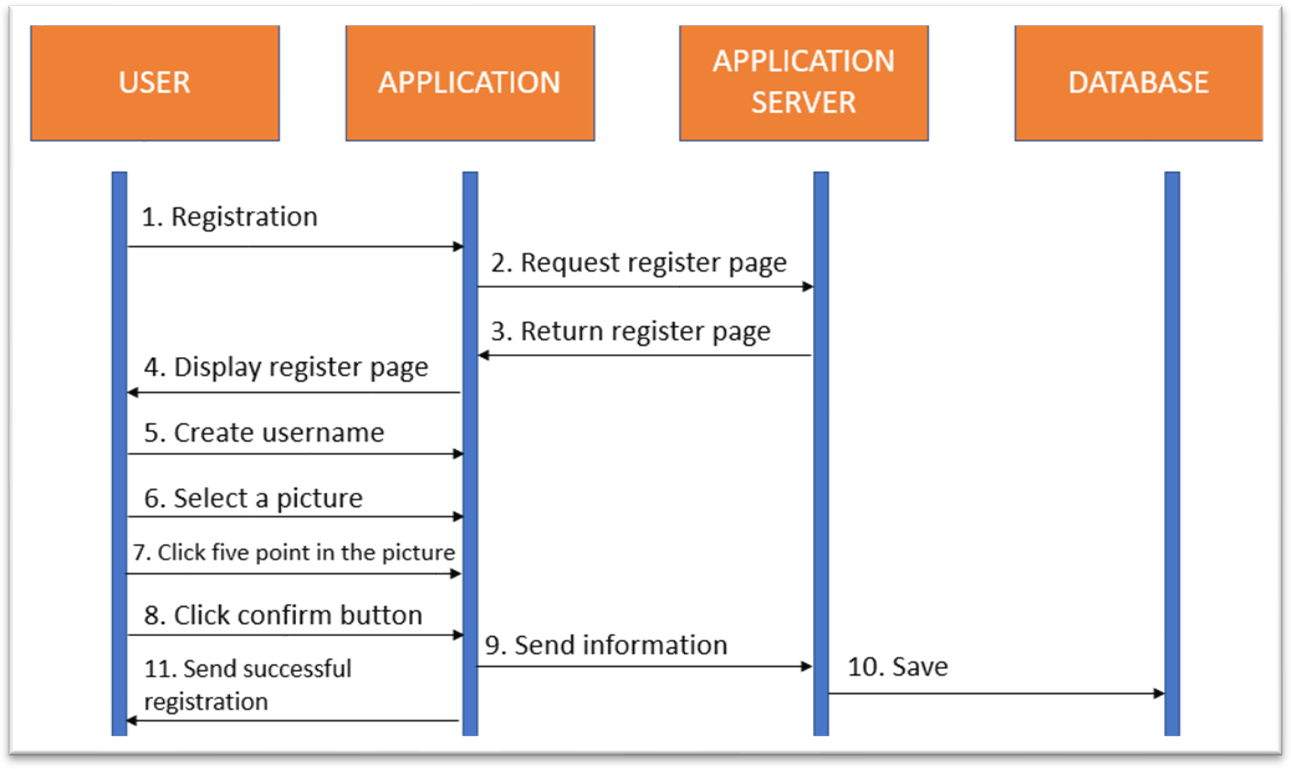


Figure 3.5: Sequence diagram for registration phase.

Figure 3.6 shows a sequence diagram of log in process. User need to make the log in by request the log in page from the server. Then, the server will return the log in page. Next, user need to enter their username and then, user will be link to page selection of picture. User need to choose one picture for their password. Next, user need to click five points in the picture which they had choose before. The picture that will return to user by the server is based on the picture that user select in the selection of picture before. After done with all the selection, user need to click on “Confirm” button. The server will response to the user by compare the current data with the data in that already register in the database. The popup message will inform the user that the log in process is success or not. If the log in process succeed, user will be link to enquiry page otherwise, the user will be link to enter username page to enable user make a log in process again.

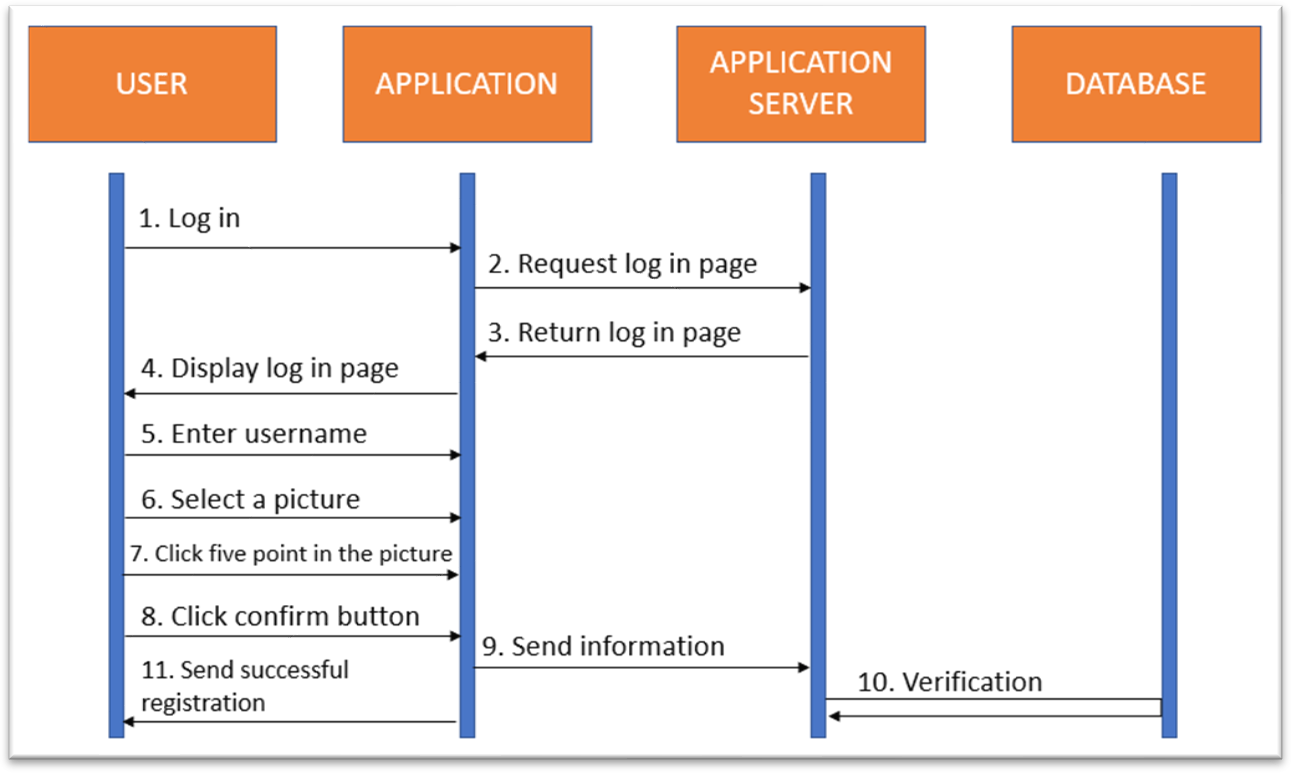


Figure 3.6: Sequence diagram for login phase

3.4 Summary

This chapter was fully describing about the methodology and requirement of the web system.

# CHAPTER 4

# IMPLEMENTATION

* 1. Introduction

This chapter discuss about the implementation and testing of graphical password authentication in web system. The implementation is the writing of code line and run the code in localhost. Meanwhile, testing phase are being used to find the bug in the system by the test with dummy input data.

* 1. User Interface of the System

There are two types of user interface (UI) which are command line and graphical use interface (GUI). In this research, graphical user interface (GUI) is implemented which means user can interact with system or software through graphical image.

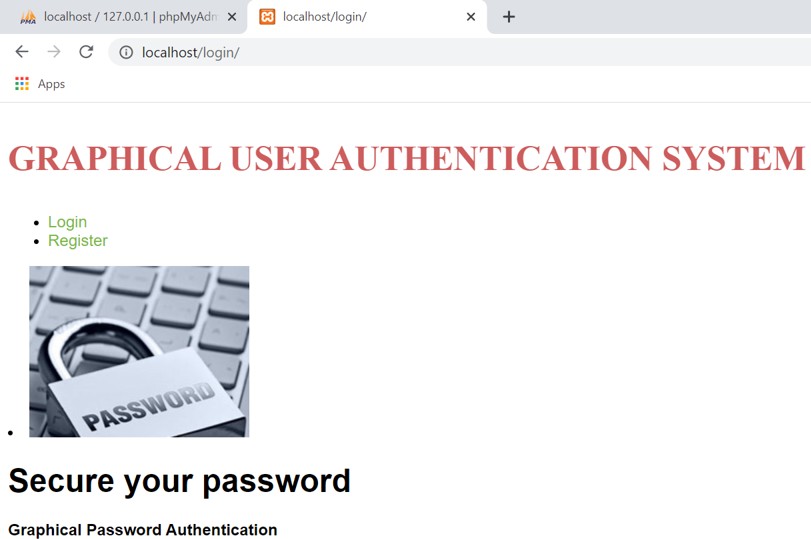


Figure 4.1: Home Interface for Graphical Password Authentication (GPA) System

* + 1. Registration Phase

Figure 4.1 shows the home interface of Graphical Password Authentication System that contains ‘Login’ and ‘Register’ link. When a user clicks on ‘Register’ link, it will redirect the user to register page which will show in Figure 4.2. In this page, a user will be asked to fill the details such as username, email and phone number. After user had fill in the details, he/she need to click on ‘Register’ button that will bring to the next page which is registrationpass. Next, user will be requested to choose a picture that represent their password out of all pictures from database show in the Figure 4.3. Then, user have to choose five clicks in the picture that had been chose which have no secret in every click than to make user remember every click as it is their password. Each of these click point will be show in Figure 4.4, Figure 4.5, Figure 4.6, Figure 4.7 and Figure 4.8 as coordinate\_1, coordinate\_2, coordinate\_3, coordinate\_4 and coordinate\_5 respectively. Lastly, user bill be directed to success\_regi page which means the user are successfully registered to the system as shown in Figure 4.9.

* 1. Summary

This shows the implementation of graphical password authentication system by using passpoints scheme. The users are given a guide step-by-step on how to register and login the system.

# CHAPTER 5 RESULT AND ANALYSIS

# Introduction

This chapter will discuss about the result and analysis of research in graphical authentication system by using pass point scheme. The result is obtained during the process of users attempt to login into the system after they going through registration phase.

* 1. User Register

Test procedure of user register and result are show in Table 1 below

|  |  |  |
| --- | --- | --- |
| Strep | Test Procedure | Result |
| 1 | <http://localhost/login/> | Home page of system |
| 2 | Click ‘Register’ link | Redirect to registration page |
| 3 | Fill up details:   * Username * Email * Phone Number | Users are able to enter their own personal details. Then users will click on ‘Register’ button. |
| 4 | Choose picture password | User choose a picture as their  password. Redirect to first click point. |
| 5 | Click first point | User click first point in page coordinate. Click ‘Next’ link for  second click. |
| 6 | Click second point | User click second point in page coordinate\_2.php. Click ‘Next’  link for third click. |

|  |  |  |
| --- | --- | --- |
| 7 | Click third point | User click third point in page coordinate\_3.php. Click ‘Next’  link for fourth click. |
| 8 | Click fourth point | User click forth point in page coordinate\_4.php. Click ‘Next’  link for fifth click. |
| 9 | Click fifth point | User click fifth point in page  coordinate\_5.php. |
| 10 | Click on ‘Next’ link. | Redirect to success register page. |

Table 5.1` Test case for register

* 1. User Login

|  |  |  |
| --- | --- | --- |
| Strep | Test Procedure | Result |
| 1 | <http://localhost/login/> | Home page of system |
| 2 | Click ‘Login’ link | Redirect to login page |
| 3 | Fill up detail:  - Username | Users required to enter a valid username. Then, they will click on ‘Login’ button which will redirect them to loginpass\_1.php  page. |
| 4 | Choose picture password. The picture must be the same as the one  that user had registered. | User choose a picture as their password. Redirect to first click  point. |
| 5 | Click first point. The first click  must be the same as during registration phase. | User click first point in page  coordinate. Click ‘Next’ link for second click. |
| 6 | Click second point. The second click must be the same as during  registration phase. | User click second point in page coordinate\_2.php. Click ‘Next’  link for third click. |

|  |  |  |
| --- | --- | --- |
| 7 | Click third point. The third click must be the same as during registration phase. | User click third point in page coordinate\_3.php. Click ‘Next’ link for fourth click. |
| 8 | Click fourth point. The fourth click  must be the same as during registration phase. | User click forth point in page  coordinate\_4.php. Click ‘Next’ link for fifth click. |
| 9 | Click fifth point. The fifth click must  be the same as during registration phase. | User click fifth point in page coordinate\_5.php. |
| 10 | Click on ‘Next’ link. | The points that user had clicks will be compared to coordinate in database with current username. If the coordinate is the same or close to the same click according to tolerance, the user will be redirect to success login page. If it is not same then an error interface  will be display. |

Table 5.2: Test case for Login

* 1. Summary

This chapter explained about the result in a system in another way, what back- end do during users are register and login into the system at the front-end.

# CHAPTER 6 CONCLUSION

* 1. Introduction

This chapter will discuss about writing a conclusion which is the final part of the research paper. Conclusion usually allow researcher to have some last words of subject which include this research project. It also allows can synthesize our thoughts and to discuss about future work.

* 1. System Contribution

Graphical password authentication implemented in web-based system is an alternative password that can replace the standard textual-based password. The objective of the system that have achieved were to design a graphical password authentication implemented in web-based system. Then to implement the graphical password authentication using passpoints scheme. Finally, to test the effectiveness of graphical password authentication system using passpoints scheme to authenticate users by using web system.

* 1. Future Work

In the future, hopefully this system can be applied in real life because it may help users that have secret or privacy account want to keep their account private and

protect their data privacy. To make this more secure, the selection of every click points might be good if they have their own character or password.

* 1. Summary

In conclusion, it is important to know what kind of algorithm are suitable for a system and the way to implement the algorithm in a system. In this proposed project, graphical password authentication by using passpoints scheme can give many benefits to users in many aspects. It will secure the users to make an authentication process in spite of the fact it takes users longer time to access into a system.

# REFERENCES

1. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. p. 26.
2. Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.
3. Ahmet Emir Dirik, Nasir Memon, & Jean-Camille Birget. (2007). Modeling user choice in the PassPoints graphical password scheme. 8.
4. Nelson, D. L., Reed, V. S., & Walling, J. R. (1976). Pictorial superiority effect. *Journal of experimental psychology. Human learning and memory*, *2*(5), 523–528.
5. Dhamija, R. (n.d.). Hash Visualization in User Authentication . 2.
6. Khan , W. Z., & Aalsalem, M. Y. (19 December, 2013). A Graphical Password Based System for Small Mobile Devices. p. 11.
7. Manjunath G, Satheesh K, Saranyadevi C, & Nithya M. (2014). Text-Based Shoulder Surfing Resistant Graphical Password Scheme. 4.
8. N.Asokan. (16 May, 2014). A Closer Look at Recognition-based Graphical Passwords. p. 13.
9. Tao, H. (2006). Pass-Go, a New Graphical Password Scheme. 11.
10. Towseef Akram , Vakeel Ahmad, Israrul Haq, & Monisa Nazir. (2017). Graphical Password Authentication. 7.
11. Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, & Pranjal Rathod. (2013). Secure Authentication with 3D Password. 7.
12. Zheng, Z., Xiyu Liu , Lizi Yin , & Zhaocheng Liu. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. 8.
13. Awais, A., Muhammad , A., M., K. H., & Talib, R. (2016). Secure Graphical Password Techniques agaist Shoulder Surfing and Camera based Attacks. 9.
14. Krishnan, S., Watkins, K.E. & Bishop, D.V. (2017). The effect of recall, reproduction, and restudy on word learning: a pre-registered study. *BMC Psychol* **5,** 28.
15. Borkar, V. S., & Golar, P. C. (2015). Click Based Graphical Passward with Text Password Authentication. *International Journal of Computer Science and Network Security*, *15*(11), 76–79.
16. Chiasson, S., Stobert, E., Forget, A., Biddle, R., & Van Oorschot, P. C. (2012). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing*, *9*(2), 222–235. https://doi.org/10.1109/TDSC.2011.55
17. Rupavathy, N., Carmel Mary Belinda, M. J., & Nivedhitha, G. (2018). A shoulder surfing resistance using graphical authentication system. *International Journal of Engineering and Technology (UAE)*, *7*(1.7 Special Issue 7), 169– 174. https://doi.org/10.14419/ijet.v7i1.7.10644
18. Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. *Scientific Research and Essays*, *5*(24), 3865–3875.
19. Science, C., & Security, I. (2008). *STUDY AND DEVELOP A NEW GRAPHICAL PASSWORD SYSTEM Dedicated to my beloved parents , my lovely wife , my children , brothers and sisters With thanks for all the years of caring , love , and support . November*.
20. Zuo, M., Zeng, G., & Tu, X. (2010). Research and improvement of face detection algorithm based on the OpenCV. *2nd International Conference on Information Science and Engineering, ICISE2010 - Proceedings*, 1413–1416. https://doi.org/10.1109/ICISE.2010.5691414