

CHAPTER 3

METHODOLOGY

3.1 OVERVIEW

This chapter explains the methodology used for research tools and environment, and presents an overview of proposed scheme. Briefly, for the development of ChoCD, the researcher used Prototyping model. This chapter also explains more about hybrid scheme, which are the combination of three graphical authentication schemes that provide the new enhancement in usability and security aspects.

3.2 PROTOTYPING MODEL

The approach that has been used to develop the ChoCD authentication scheme prototype is the Prototyping model. It is the most suitable model, because of its ability to incorporate changes and new features in future according to Figure 3.1.

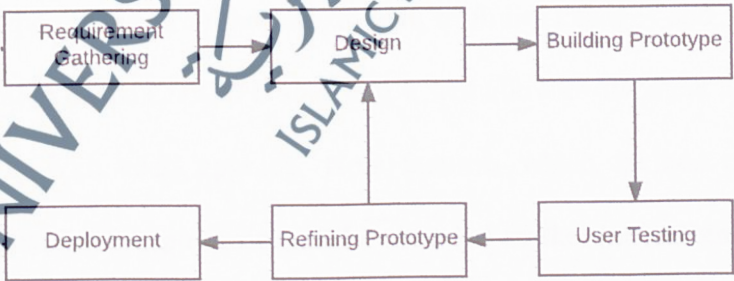


Figure 3.1: Prototyping Model

This model is an engineering technique that has been transferred to computer systems development. It suggested using a small-scale model of the proposed system so that

users can give feedback and ensure it meets thesis objective. By using this prototype, the user can get an “actual impression” of the system, since the interactions with prototype can enable the user to better understand the requirements of the desired system.

3.2.1 Development Phases

In this phase, the development of ChoCD prototype need to complete through all of six phases, there are:

1. **Requirement Gathering:** The requirement phase in this project is the first phase of the whole development process. It involves the identification of the requirements analysis of the system. In getting the requirements for the system, information gathering through the study of existing system would be analysed from previous research papers that related to authentication system as discussed in Chapter 2. This is important because it measures how well they will embrace the proposed system.
2. **Design:** Next phase of the development is system design. In this phase, it is very important to keep the design open to future changes and improvements. The design of the ChoCD is such that it will allow evolvement as new features come in with each upgrade. New features which include additional test processes. Less importance will be awarded to the documentation and more attention to the usability, security and the ability for the system to deliver the desired output with minimal time consumed.
3. **Building Prototype:** This phase is strictly for programming. It involves the process of converting a system specification into an executable system. It is a

very key process in the overall process of system development. This is the phase where the system developed by using the hybrid scheme.

4. **User Testing:** The ChoCD authentication prototype is tested by a random user to make sure it meets with the requirements. In this phase, the prototype of authentication system was verified and tested if it matches with the described system in the documentations. After that, the user that participated in the testing process was validated the result based on given questionnaire. Explanation on the participants' feedback and analysis of the result would be explained further in Chapter 5.
5. **Refining Prototype:** Based on the feedback from the survey on the questionnaire at user testing phase, the researcher refines back the prototype of the authentication scheme. By doing refining process, it elevates this proposed scheme towards productivity in term of usability and security.
6. **Deployment**

This is the final stage, which involves the whole system deployment, maintenance and operations. Once the ChoCD authentication prototype has been completely developed, it would be deployed into the potential systems that need authentication process.

3.3 DEVELOPMENT TOOLS

The development process of ChoCD authentication scheme used the following software as shown in Table 3.1:

Table 3.1: Software and tools used in the development and testing

Software	Function
PHPDesigner	phpDesigner 8 is a fast and powerful PHP IDE and PHP editor with full-blown HTML5-, CSS3- and JavaScript built-in editors. Highly customizable IDE with intelligent syntax highlighting, debug support, syntax analyzing, support for object-oriented coding, code insight on the fly, code templates, code snippets, todo and bug managers, work with projects and frameworks, intuitive code navigation, code formatters and minifiers and all wrapped into a nice looking intuitive user interface.
PhpMyadmin	phpMyAdmin is a free and open source tool written in PHP, intended to handle the administration of MySQL with the use of a web browser. It can perform various tasks such as creating, modifying or deleting databases, tables, fields or rows; executing SQL statements; or managing users and permissions.
MAMP	MAMP is a solution stack composed of free and open-source and proprietary commercial software used together to create an own server and run dynamic web applications.
Internet Browser	It used to access information provided by web servers in private networks or files in file systems. The major web browsers are Firefox, Internet Explorer, Google Chrome, Opera, and Safari.
LucidChart	Lucidchart is online diagram application that makes it easy to sketch and develop flowchart diagrams for system development.
Microsoft Excel	Provide function to analyse data. It is a

	spreadsheet developed by Microsoft. It features calculation, graphing tools, pivot tables, and a macro programming language called Visual Basic for Applications.
--	---

3.4 COMBINATION OF THREE GRAPHICAL AUTHENTIFICATIONS

In this thesis, the combination of three graphical authentications, namely hybrid scheme is used to develop the prototype of graphical password authentication scheme. The hybrid scheme is based on users’ action when they authenticate into the system; choice-based, click-based, and draw-based. The idea could be constructed quite simple and straightforward. Then, it not only guides the user to master this scheme with ease, but also makes the whole system easy to implement. Figure 3.2 shows the idea of this work. Users should just choose two graphical images, click then draw the pattern on the point on it as the login password. The whole process includes two main steps: password creation step (registration) and the authentication step (login). Variants of the proposed authentication scheme will be introduced in the further description.



Figure 3.2: Mapping from choice-based to click-based and to draw-based

3.4.1 The Illustration of Proposed Graphical Authentication Prototype

Figure 3.3 shows the initial design of authentication system prototype. The illustration includes registration and login phase. This is the main part of the authentication scheme, which is the evaluation of usability and security were analysed. To meet the

usability requirements, the design of the interface was easy for user to use and manage.

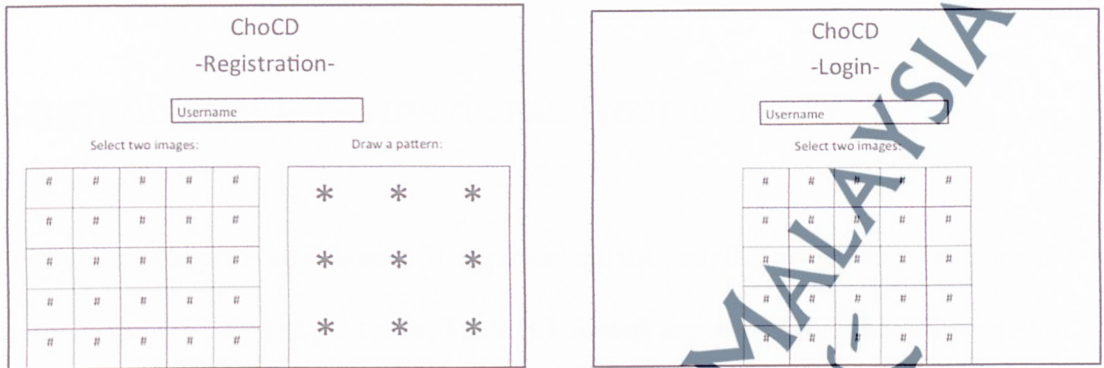


Figure 3.3: Initial design of proposed graphical authentication prototype

For the graphical images selection in first authentication, the proposed scheme provided 25 random images in 5x5 grid form. For this prototype, the participants were needed to choose two images from the fruit theme. These images were chosen because they were common images in daily life which were easy to recognize and remember (Vrunda, 2013). The images in this grid will be generated randomly for every time when user login and make a registration into the system. This type of system requires users to rely solely on recognition of the selectors and not on the recollection of positions of the locations of those selectors on an input device (Jonathan, 2015). This part of authentication offers security through large password space and high usability as the user has to recognize a number of images (Umar & Rafiq, 2012).

During the authentication phase, this scheme will ask user to choose graphical images. Then the user needs to click a point and start to draw a pattern on the screen as a combination of password. Based on combination of those actions, it makes the authentication system more secure (Gao et al., 2010). This feature significantly

enhances the password space and thus resulting in increased security. While, in term of usability it will ease the user to choose their images rather than to remember the long text-based password.

3.5 METHOD OF EVALUATION ON PASSWORD ENTROPY

Since the security of any password depends on the length, giving any reasonable-length passwords in a 5x5 grid as in Table 3.1, it was confirmed that the full password entropy for the authentication scheme is more than that of the full textual passwords space with keyboard input characters (Obasan et al., 2013). It is because the number of password entropy would be multiply by the number of 'secret', x :

$$x * (\log_2 N) \tag{2}$$

The password entropy for 6x6 grid stated in Table 3.2 provides a better value. However, it had a limitation in usability aspect. For this reason, in ChoCD development 5x5 grid was a suitable grid size. Below is an example of the password entropy calculation by using formula (2):

$x = 1$ (number of secrets)
 $N = 2$ (size of grid)

$1 * (\log_2 2) = 2 * 2 = 2_{\#}$

Table 3.2: Comparison of grid size

Grid Size ($x^2=N$)	Password Entropy Possibility ($\log_2 N$) (bits)
2 x 2 = 4	2
3 x 3 = 9	3.17
4 x 4 = 16	4
5 x 5 = 25	4.64
6 x 6 = 36	5.17

3.6 QUESTIONNAIRE SURVEY

To conduct evaluation on the developed prototype, the questionnaire was distributed to the participants after they had done testing the prototype. This questionnaire was adapted from the previous research in graphical authentication scheme that was Implicit Password Authentication Scheme (IPAS) by Almuaini et al., (2013). For this questionnaire, on demographic information, participant’s education background was asked. Then, the questionnaire is divided into two main parts: general information about graphical authentication schemes and ChoCD evaluation after performing the testing.

The category on general information about authentication schemes included the three following questions: For the first question, “how frequently do you deal with the authentication schemes?” Response options for this question were always, usually, often, rarely and never. The second question was “how do you evaluate the ChoCD from an ease-of-use perspective?” Response options for this question were a rating from 1 to 5 where 1 is very easy and 5 is very difficult. The ChoCD evaluation category includes ten questions, which cover the main and minor factors. The

response options for questions 1 and 2 were similar to those for questions 1 and 2 in category one. For the third until tenth question were about the detail of ChoCD authentication system prototype as attached in Appendix C.

3.7 METHOD OF DATA ANALYSIS

As mentioned in Section 3.4, before conducting the user study, password entropy for ChoCD authentication scheme was calculated and compared with existing popular graphical authentication; Windows 8 graphical authentication, Android pattern lock and online banking system. This evaluation was discussed in Chapter 5, Section 5.2.1.

The participants were invited to experience ChoCD prototype for two separate occasions. In the first week, the researcher introduced and gave some overview of ChoCD prototype to the participants. After that, they used and tested ChoCD for the first time. Then, two weeks later, the researcher asked participants to use this prototype again to test either they still remember their password or not. Finally, the questionnaire survey was distributed (refer Section 3.5) and all of the collected data were analysed and presented in Chapter 5. The purpose of analysing data was to obtain usable and useful information. The analysis described and summarised the data, identified relationships between variables, compare variables and identified the difference between variables. In this thesis, the analyses of data collected were based on ordinal scale as measurement scale that used in ChoCD questionnaire survey. By using ordinal scale, the data can be classified into non-numerical or named categories an inherent order exists among the response categories. Ordinal scales were seen in questions that call for ratings of security (i.e. not secure, secure, moderate, very secure

and strongly secure) and usability (i.e. very difficult, difficult, moderate, easy and very easy).

3.8 SUMMARY

This chapter covered the methodology used in the development of ChoCD authentication scheme, environment, and overview of proposed scheme. Prototyping model were used as method to developed ChoCD. This chapter also explained the hybrid scheme, which are the combination of three graphical authentication schemes and finally the initial design of proposed scheme. After our initial survey on previous graphical passwords, it is anticipated that the hybrid scheme offered the most promising alternative among those proposed so far. The next chapter further explains on the development of ChoCD, which is the main part in this thesis.