GRAPHICAL PASSWORD AUTHENTICATION FOR CHILD PERSONAL STORAGE APPLICATION

1Tay Yi Yang, 2Palaniappan Shamala, 3Muruga Chinniah, 1Cik Feresa Mohd Fozzy

1Faculty Computer Science & Information Technology, University Tun Hussein Onn Malaysia, Johor, Malaysia.
2Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Johor (UiTM), Segamat, Johor, Malaysia
3Faculty of Business Management, Universiti Teknologi MARA (UiTM), Segamat, Johor. Malaysia
shamalap@uitm.edu.my

Abstract. Mobile applications are very popular among the children nowadays as children use it for many purposes such as entertainment, learning or education. Keeping hand written notes in hard copy is not a good choice as the accumulated papers would mess up child’s study space. Although there is high adoption of mobile application among children nowadays, but children are not educated to practice password to secure their personals in their primary school syllabus. Therefore, an application which can provide personal storage for children to store their notes in softcopy forms called Graphical Password Authentication for Child Personal Storage Application was proposed. The adoption of graphical password authentication in the proposed system is intended to cultivate children practice password to secure their files in an interesting method. The proposed system is developed in Android mobile application platform and the Object-oriented Mobile Application Development is applied as methodology of the project. The proposed system’s functional requirements are implemented according to user’s requirements and the application interfaces implementation also based on user’s characteristics that has been studied in literature reviews. The significance of the project is awareness on secure file keeping among the children. Children can use graphical password in their childhood age would be the advantage for them in the future because they would make a sense to protect privacy by setting up password. In terms of information security, the proposed system has mentioned some values that would be achieved which are authentication, confidentiality and availability.

Keywords: Mobile Application, Graphical Password, Secure File, Authentication

1. Introduction

Living in this information technology era, children nowadays needs to digest more knowledge and information during their education process. They are always provided with educational materials as a...
source of knowledge and practice. Childs keeping all the education documents in the traditional method like hand-written notes. Digital form of documents keeping method can replace traditional method because many things in this world are digitalized to ease the burden of people in daily life. Computerized is essential system to keep files in a convenient way and systematically.

There are shortcomings and problems are identified where children in primary school having difficulties in keeping their files securely. As children’s education age go on, they would get more files and stacks of paper to be kept. An alternative method which is keep their hand-written notes in soft copy form is suggested as a convenient way to store hand-written notes systematically. Since mobile application adoption among the children are increased gradually in recent years, hence it would have a potential to create an application which allow children to store their handwritten notes in softcopy form by taking photo on the notes and they can access the hand-written notes through the mobile application.

Children have the ability to be nurtured to store files digitally as a research found that nowadays children are capable to use portable devices to watch films, videos, including streaming, on-demand and catch-up services (Jackie Marsh, 2015). Children are necessary to have the mind set of setting up password or a defend base for the information that they want to store. Graphical password will be the alternative.

As children already started to learn to recognize the shape of alphabet and some simple new words in their starting point of education process (Robertson, 2007), they are more suitable to have graphical password authentication in the proposed system rather than text based password. In order to overcome these problems, Graphical Password Authentication for Child Personal Storage Application was proposed. The main objectives for the proposed application are as follows:

1) To design graphical password authentication for child’s application.
2) To implement the proposed system by using Object-Oriented Mobile Application Development Methodology.
3) To test the functionalities and user acceptance on proposed system.

Graphical Password Authentication for Child Personal Storage Application is proposed to provide a space for children to keep their hand-writing notes in image file formats securely. Children will have practiced to save their personal data in a secure way. In terms of information security, the proposed system has mentioned some values that would be achieved which are authentication, availability and confidentiality.

The great importance is to cultivate the child’s awareness in the securing their personal files. Children should learn on how to keep their files securely using password. Living in the global of information technology which is rapidly growth, children should be cultivated with the awareness of privacy in files securing.

The paper is organized as follows: Section 2 will discuss the related works which related to proposed system. Section 3 discuss methodology that has been used to develop the Graphical Password Authentication for Child Personal Storage Application. Section 4 discusses the result and discussion. Finally, Section 5 concludes the work.

2. Related Works
This section discusses the literature review of child’s capabilities in recalling and recognizing the graphics and explains in detail the graphical password techniques, its description and pictures. Moreover, the characteristics for graphical password for child system is studied. Finally, the difference between three types of existing system had been study and compared with the developed system.

Child’s Capabilities in Recalling and Recognizing the Graphics
The adoption of mobile application among the children are gradually increase. Children use mobile application for education purpose as there are lots of resources can be found in digital formed (Papadakis, 2017). According to a research of children’s mobile adoption in European and Asia countries, it’s found that the children with range age of 10 to 12 years old are the most common age to
receive their first mobile phone (GSMA, 2014). In Malaysia, a child starts primary education in the age of 7 years old and end in 12 years old (Mutalip, 2013). Mobile application designed to solve the problems according to specific of user (Thornton, 2018). Therefore, the proposed project was developed for child in Malaysian’s primary education age range (Mutalip, 2013).

It is necessary to determine the capabilities of child in applying the graphical password authentication method before the designation. Generally, there are two factors were taken into the consideration, that are, eyesight capability and memory capability.

a. Eyesight capability: Child must be able to have a clear vision to look at the display screen of graphical password authentication. It is undeniable, colour-blindness issue should take concern on the child. Colour-blindness patient have deficiency in recognizing certain colour. A research has found that 3.9% of children defect with colour blindness over the amount of 2001 children with average age of 10 which are being tested (Shrestha, 2010; Shrestha 2016). Therefore, author Gao (2009) advising to design the graphical password based on no colour recognition to ensure the individual with colour deficiency would be not restricted to use the system.

b. Memory capability: The children would tend to forget and fail to recall and recognize their graphical password and caused them to end up with wasting time to recovery their password (Imran, 2016). Child facing difficulty to recall and recognize too many number of graphics according to their current memory capabilities. Adults perform better in critical thinking. Therefore, adults would have their own strategy to remember their selected password. While, child only able to choose and select the graphical password based on their interest due to their poor meta-memory compare to adult (Pacchioli, 2005). Author Stobert (2017) recommend that child can be given to remember 2 number of graphics without graphic sequences.

*Graphical password authentication*

Graphical password is a type of password that use image, draw or clicks on correct region as input scheme. Graphical password is an idea given by Blonder in 1996 which states that to authenticate through graphical password, an image that appear on screen and user should clicking on the area of image to select the correct regions (Blonder, 1996).

Graphical password authentication is mainly categorized as two which is Recognition based technique and Recall based technique.

a. Recognition based technique shall have numerous images are show to user at registration phase (Masrom, 2009), images are randomized. According to the predefined condition, user has to select the images as password input.

b. Recall based technique has its subcategory which is pure recall based technique such as Passdoodle or drawing motion technique. The another subcategory is cued recall based technique such as pass point, Pass-Go, Drawing Geometry, Blonder and Passlogix V-Go technique (Ramanan, 2014).

Table 1 shows that Graphical password authentication has several of techniques.

| Technique       | Description                                                                 | Example Picture |
|-----------------|-----------------------------------------------------------------------------|-----------------|
| Dhamija and Perrig | In this techniques, user will be given grids of images. From these images, user have to select some of 5 of them as the predefine image. During the login phrase. User would undergo authentication by random images and user has to select the predefined images to pass the authentications (R. Dhamija, 2000). | ![Example Picture](image.png) |
| Technique | Description |
|-----------|-------------|
| **Passface** | Human faces is used as the image for authentication. In the predefine phrase, user needs to defined 4 faces as pass-words. During login phrase, a set of nine human faces will display in grids of 3 x 3, only one correct face inside a particular set. The user would be authenticated with four sets of pass faces to qualify as a successful authentication (Passface, 2007). |
| **Draw-a-Secret (DAS)** | User is required to re-draw the predefined picture on a 2-D grid. The user is successfully authenticated when the drawing touches the same grids in the same sequence (Xiaoyuan Suo, 2005). |
| **Story with DAS** | User is required to draw curves or line over the grid of images according to the image sequence which is predefined during the registration phrase. The sequence of image selected represent the story line of the graphical passwords (Haichang Gao, 2010). |
| **Convex hull** | User need to recognize the pass objects and forms the convex hull. To make the password difficult to guesses, user can increase number of object to be select to form a larger convex hull but it will make the display very crowded and objects almost indistinguishable (S. Wiedenbeck, 2005). |
The proposed system should have an authentication interface that is fulfilled child-friendliness characteristics to raise the child’s interests in the adoption of graphical passwords. Table 2 shows the result of study (DrinTeam, 2018) (Lazaris, 2009) (Kraleva, 2017) on characteristic of graphical password for child. Dhamija and Perrig technique of graphical password is applied in the proposed system because graphical password with recognition based matches for children. Hence, would best for the child.

Table 2: Characteristic of graphical password for child

| Characteristic                                      | Description                                                                 |
|----------------------------------------------------|-----------------------------------------------------------------------------|
| Recognition based technique                        | Recognition based technique only require child to identify which of the images has been predefined previously. |
| No need to recognized and recall the sequences of the predefined image | The sequence to select the images would burden the memory capability of child which would cause children always forget their own graphical password. |
| Easy password recovery                              | It is possible that user forget their password. Child’s graphical pass-word should easy to recover to ensure the learning process is not delay due to authentication issues. |
| Simple login step                                   | Single authentication process with graphical password is enough for children to complete log in process. |
| Large functional button                            | The clickable and interact able buttons and areas must fit with or larger than child’s fingers to avoid false clicking or tapping on screen. |

Comparison of proposed system and existing system

The output of the comparison is important to determine the differences between the existing systems and clarify how the proposed system can best achieve the user-friendliness to the targeted user. This section describes and elaborates in detail by comparing three similar systems which are password manager, graphical image password and GsecuRe Application. The comparison between existing system and proposed system is show in Table 3 to clarify their similarities and differences.

Table 3 Comparison of existing system and proposed system

| Characteristic                  | Password Manager | Graphical Image Password | GsecuRe | Proposed System |
|--------------------------------|------------------|--------------------------|---------|----------------|
| Android mobile application     | Yes              | Yes                      | Yes     | Yes            |
| Graphical password authentication | Yes             | Yes                      | Yes     | Yes            |
| Mini game                      | No               | No                       | Yes     | Yes            |
| Support multiuser account       | No               | No                       | Yes     | Yes            |
| More than one functional application | No             | No                       | No      | Yes            |
| Cloud storage                  | No               | No                       | No      | Yes            |
| Graphical password specially for child | No             | No                       | No      | Yes            |

Our proposed mobile application for child personal storage is differing than other system in such a way that allow user to upload, delete and download the files within a storage space. According to Kraleva (2017) child will lose their interest and confidence to deal with application that are too complex to handle. The proposed system has function to create users own graphical password, manage their image files, keep their learning notes and explore the system by learning how to manage their own education notes as they can upload and delete their files inside the application. Children will practice to save their personal data in a secure way. Child always expect more from the application that they would like to explore. Some simple but surprising functionality such as mini games was added to attract child’s interest so that they can keep on using the application.
3. Methodology

This section discusses the methodology that has been used to develop the Graphical Password Authentication for Child Personal Storage Application that is Object-oriented Mobile Application Development (OOMAD) methodology. OOMAD methodology enables the developer to carry out any changes at any phase in order to achieve the objectives of the project. System developer able to make changes on each of the phase in a scalable and flexible way based on necessities and challenges in the whole development process. The OOMAD methodology consists of phases in which the proposed model is discussed and refined by the target user, then it is implemented by developer.

Figure 6 show the process of OOMAD Model and clearly illustrate how this methodology works in the process of deployment the proposed system. The main five phase of the methodology are requirement analysis, planning and design, development, testing and deployment. Requirement analysis defined the problem and planning requirement of the system. Planning phase is a process to digest all the information gained from requirement phase and start to create the choices of decision in term of interface design, applicable technology, programming language and the arrangement on how to works against the constraints like time, cost, scope and quality. Design phase considers the design of mobile application into two aspects which is user interface design and implementation design. After the system has fulfilled all the requirement in planning and design phase, the system developer will have a smooth development phase as the developer just need to follow what is decided on the design phase. Testing is performing to ensure the proposed system work well before the deployment phase.

A. System Analysis & Design

System analysis & design explains the overall process and system architecture of Graphical Password Authentication for Child Personal Storage. System analysis & design is a sketch of the system interface before the actual system development in order to provide clear and visualize of functionality and work flows of the proposed system.

Use case diagram is applied to the analysis process to capture the requirements of the proposed system. Four use case and the environment of the system is illustrated in Figure 7.
Class diagram is applied to visualize the relationship between the classes in the proposed system. The relationship between the classes is important to clarify to avoid misconfiguration of system functionalities during the implement process. Seven classes are determined for the system which are signup, login, profile activity, application menu, image file management, mini-game, diary and DatabaseAPI class. Each class performs different activity. Signup responsible for registration handling, login is responsible for user sign in, profile activity responsible for user information details, application menu responsible for menu display, image file management and mini-game are responsible to preform respective activity handling and DatabaseAPI class is responsible to communication between application and database server.

System design discuss the design of system architecture, security architecture and interfaces of Graphical Password Authentication for Child Personal Storage system. Proposed system architecture contains two parts, known as authentication module and application modules. Graphical password authentication is applied to replace the text password input method in login and registration interfaces. Authenticated user is allowed to use the application modules, such as image file management application and mini games. The proposed system use cloud storage API for user’s image files storage and No SQL database services.

User need to provide credential to pass the authentication. Database API is important to verify the credentials input by the user. A session is important to store user information and allow user to access the multiple resources page legitimately. The single user interface session is destroyed after user has logged out from the system. Figure 8 shows the security architecture of the proposed system, used to authenticate the legitimate user.
The five significant interfaces for the proposed system are registration interface, login interface, user profile interface, image file management interface and mini game interface.

B. Implementation and Testing

In system implementation phase, Android Studio and Firebase mobile application development platform are used to implement the functional requirements of the proposed system. Firebase is a mobile and web application development platform that provides backend supports to an application (Khawas, 2018). The proposed system is an Android mobile application written in Java programming language. The description for module are shown in Table 4 and the following figures, Figure 9, 10 and 11 are system modules interfaces.

| Module | Description | Picture |
|--------|-------------|---------|

Table 4: The descriptions for Module
| Module                     | Description                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| User Registration Module  | New user is required to register before start to use the application. Registration process requires user to input email and select graphical password. |
| User Login Module         | Each user needs to login the system before start using the application as to ensure the authority of the user. Login process requires user to enter email and choose user predefined graphical password |

Figure 9: User Registration Module

Figure 10: User Login Module
Image files management module is the main module of application which allow user to upload and delete the image files.

The proposed system’s testing includes functional testing, user testing on proposed system’s functionalities and user acceptance testing. The system testing conducted to ensure all modules function as expected. This is to determine whether the system has been developed achieved the objectives and user requirement. The test phase was conducted to prove that the design of each phase has been achieved. In addition, the test system is also intended to identify weaknesses in the system and find solution to overcome those weaknesses.

A set of questionnaire is prepared and delivered to target users to test the proposed system. This is done to collect user’s feedback, comments, bugs and suggestions for improvement. The determination of user’s ability to use the proposed system’s functionalities is carried out by given them to use the proposed system. There are 50 (N) respondents, who age range of 7 to 12 willing to become the volunteers to test the system according to the test cases. Table 5 shows the results of user testing on proposed system.

Table 5: Test report of user testing on proposed system’s functionality.

| No. | Test Case                                           | Expected Result         | Actual Output            |
|-----|----------------------------------------------------|-------------------------|--------------------------|
| 1   | Ask user to register as user of proposed system.    | All user succeed.       | 46 out of 50 succeed.    |
| 2   | User able to register within one minute.            | All user succeed.       | 48 out of 50 succeed.    |
| 3   | Ask user to login the application after registration.| All user succeed.       | As expected.             |
| 4   | User able to login within one minute.               | All user succeed.       | 47 out of 50 succeed.    |
| 5   | Ask user to come again for login one more time after 15 minutes. | All user succeed. | As expected.             |
| 6   | User able to upload the image files to their storage space. | All user succeed. | As expected.             |
| 7   | User able to delete the image from storage space.   | All user succeed.       | As expected.             |
| 8   | User ask to logout from the system.                 | All user succeed.       | As expected.             |
The proposed system has passed the user testing evaluation. Each respondent is given experience to use the proposed system and majority of the respondents are able to use the proposed system easily. The functionalities of proposed system have fulfilled the user requirements according to the user test output.

Four (4) questions were asked in the survey. The results for the questionnaire is presented in Table 6. The percentage achieved for each aspect are more than 50%, in which we can conclude that more than 40 respondents out of 50 agreed that the proposed system is user-friendly, all the module is acceptable, and interactive interface.

Table 6: User acceptance report for proposed system

| Evaluated Aspects | Result (N=50) | Percentage of agree |
|-------------------|--------------|---------------------|
| Graphical password of proposed system is user friendly to respondents | 47            | 94%                 |
| Soft copy files keeping method in learning is high supported among the respondent. | 45            | 90%                 |
| The proposed system is user-friendly to respondents. | 46            | 92%                 |
| The interfaces design of proposed system is acceptable and user-friendly to respondents. | 43            | 86%                 |

5. Conclusion

Graphical Password Authentication for Child Personal Storage Application provide a space for child to manage their notes such as short-notes and important study notes securely. The child will be introduced with an image file keeping application and simple graphical password authentication. They will practice to save their personal data in a secure way.

The proposed system requests the credentials from user before access to the services provided by the system, the value of authentication is achieved. The value of availability also could be achieved through the proposed system as cloud storage technology adopted in the proposed system allow the user to access to their image files based on demand in the condition of internet access. Confidentiality also included in the proposed system through the adoption of graphical password method to reduce the risk of password being exposed during the login session.

The great importance is to cultivate the children’s awareness in the field of information technology. Text password always not the only shield to protect the confidential information since we have the alternatives. Graphical password provides an easy-to remember but hard-to-guess solution for a system authentication of covered information which eases the human memory capability. Especially for the children, use pictures as a password would solved the problems of words limitation. In the nutshell, the proposed system can cultivate children to the importance of keeping their image files securely using the password. Through the practices of the system, children will learn to be independent in keeping of digital documents securely.

Acknowledgement

This research is supported by Universiti Tun Hussein Onn Malaysia under Tier 1 Grant Scheme Vot H237 and Vot H101.

References

Blonder, G. E. (1996). Graphical password. U.S. Patent 5559961. Murray Hill: Lucent Technologies, Inc.

DrimTeam. (2018). 10 Golden Rules of Interface Design for Children. Retrieved from Drimlike: https://www.drimlike.com/en/blog/10-golden-rules-of-interface-design-for.html
Gao, H. (2009). Design and Analysis of a Graphical Password Scheme. *Innovative Computing, Information and Control (ICICIC)*.

GSMA. (2014). Children’s Use of Mobile Phones. Special Report 2014, 523-531.

Haichang Gao, Z. R. (2010). *A New Graphical Password Scheme Resistant to Shoulder-Surfing*. P. R. China: Xidian University.

Imran, A. (2016). *An Exploration of Graphical Password*. Canada: School of Computer Science, Carleton University.

Jackie Marsh, L. P. (2015). Young Children (0-8) and Digital Technology. UK: London School of Economics and Political Science.

Kraleva, R. (2017). Designing an Interface For a Mobile Application Based on Children’s Opinion. *International Journal of Interactive Mobile Technologies*, 11(1), 53-70.

Khawas, C. (2018). Application of Firebase in Android App Development-A Study. *International Journal of Computer Applications*, 49-53.

Lazaris, L. (2009, November 2009). *Designing Websites For Kids: Trends And Best Practices*. Retrieved from Smashing Magazine: [https://www.smashingmagazine](https://www.smashingmagazine)

Masrom, F. T. (2009). A Survey on Recognition-Based Graphical User Authentication Algorithms. *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, pp. 119–127.

Mutalip, H. (2013). Overweight among primary school-age children in Malaysia. *Asia Pacific Journal of Clinical Nutrition*.

Passface. (2007). *Real User Corporation*. Retrieved from Passface: [www.passfaces.com](http://www.passfaces.com)

Pacchioli, D. (2005). *Probing Question: Do children have better memories than adults do?* Penn State: Infant Brain Development and Cognition Laboratory.

Papadakis, S. (2017). Mobile educational applications for children: What educators and parents need to know. *Int. J. Mobile Learning and Organisation*, 11(3).

R. Dhamija, a. A. (2000). *Déjà Vu: A User Study Using Images for Authentication*. 9th USENIX Security Symposium.

Ramanan, S. (2014). A Survey on Different Graphical Password Authentication Techniques. *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, issue 12, pp. 7594–7602.

Robertson, R. (2007). Understanding and nurturing young children’s writing development. *Child Care Exchange*, 40-44.

Stobert, E. (2017). Teaching Authentication in High Schools: Challenges and Lessons Learned.

S. Wiedenbeck, J. W. (2005). Design and longitudinal evaluation. *International J. of Human-Computer Studies* 63, 102-127.
Shrestha, R. (2010). Color Vision Defects in School Going Children. *Journal of the Nepal Medical Association*, 264-266.

Shrestha, S. (2016). A Universally Designed and Usable Data Visualization for A Mobile Application in the Context of Rheumatoid Arthritis. *International Journal of Advanced Computer Science and Applications*, 7.

Thornton, L. K. (2018). Specific features of current and emerging mobile health apps: user views among people with and without mental health problems. *mHealth*, 56-56.

Xiaoyuan Suo, Y. Z. (2005). *Graphical Passwords: A Survey*. 21st Annual Computer Security Applications Conference.