A Hybrid Graphical User Authentication Scheme in Mobile Cloud Computing Environments

Khalil H. A. Al-Shqeerat[1], and Khalil Ibrahim Abuzanouneh[2]

[1]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia
[2]Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia

***Abstract*:** User authentication is a critical security requirement for accessing resources in cloud computing systems. A text-based password is a standard user authentication way and it is still extensively used so far. However, textual passwords are difficult to remember, which forces users to write it down and compromise security. In recent years, graphical user authentication methods have been proposed as an alternative way used to verify the identity of users. The most critical challenges cloud-computing users face is to post their sensitive data on external servers that are not directly under their control and that can be used or managed by other people. This paper proposes a question-based hybrid graphical user authentication scheme for portable cloud-computing environments. The proposed scheme comprises advantages over both recognition- and recall-based techniques without storing any sensitive information on cloud servers. The experimental study and survey have been conducted to investigate the user satisfaction about the performance and usability aspects of the proposed scheme. The study results show that the proposed scheme is secure, easy to use, and immune to potential password attacks such as brute force password guessing attacks and shoulder surfing attacks.

***Keywords*:** Security, Cloud Computing, Authentication, Graphical Password, Recognition Technique, Recall Technique**.**

1. Introduction

An authentication process is a critical security requirement for any remote system. It determines whether a user can access services or not. Nevertheless, most cloud computing systems still rely on the conventional alphanumeric password with its hashed value to authenticate an identity of a legitimate user and control his access to resources. A classical textual password has significant security and usability problems [1]. Attackers may guess or obtain the weak and short-length password using a variety of ways such as brute-force, dictionary, or any other password-cracking common attacks. Users can pick a complicated long-size password to avoid guessing attacks. However, the strong password is often hard to remember, which forces users to write it down on an external sheet or store it in their smartphones or into a computer file.

Graphical-based passwords have been proposed as an alternative potential solution to overcome text-based problems, mainly because humans can better recognize and remember visual information than text-based string. Initially, the graphical password was presented in [2], in which an image appears on the screen, and the authentication server allows users to select a few predefined regions. Once users choose the correct regions, their identities will be verified successfully. A graphical-based password enables a user to remember a complex large-size space password. The space size of the graphical password is considerably higher than the conventional password due to a large number of possible images used [3].

Furthermore, the graphical password could also resist dictionary attacks, since it depends on the mouse input in place of the keyboard, as there are almost no searchable dictionaries already exist to launch dictionary attacks. Nevertheless, graphical-based passwords take more time than classical textual passwords since the user has to go through a long process by selecting many images or following a series of predefined points in order.

Generally, graphical passwords are divided into two main categories, recognition-based and recall-based authentication techniques [4]. In recognition-based, a set of images is presented to users, in which the authentication is accomplished by prior detection and identification of the selected images during the registration phase. While, in recall-based, the user must re-submit something that he/she had picked in advance.

For cloud computing authentication systems, graphical authentication problems must be addressed in-depth to overcome security and usability aspects to effectively secure cloud systems [5]. Many security flaws in web-based environments emerged when implementing graphical authentication systems [6]. The server could be secured in such web environments, while the client machine may have a set of potential security vulnerabilities that would breach the graphical authentication system. Moreover, some graphical authentication schemes use the same images for any feasible input, which makes them vulnerable to attackers [7]. For example, PassFace technique has a short-space password in which users often pick predictable and weak graphical passwords when selecting the same click points in the image.

This paper aims to provide a reliable, easy to use, and secure authentication technique appropriate for mobile cloud computing environments. The proposed hybrid graphical user authentication scheme incorporates benefits over recognition-based and recall-based techniques without storing any confidential information on cloud computing servers.

The rest of this paper is structured as follows. Section II covers some recent research literature related to the proposed authentication scheme. Section III elaborates on the design of the proposed work. Section IV analyzes the security features and usability of the proposed scheme. Section V implements the authentication scheme and discusses the results obtained by conducting an experimental study.

2. Literature Review

Several of graphical-based authentication schemes have been suggested in the last decade. This section focuses on some research related to the proposed scheme.

In [8], Shraddha et al. have suggested a way for selecting a username and set of images as a password in the cloud environment. It provides a graphical password based on the alphabet series position of characters in the given username.

A secure authentication method using a graphical password has been proposed in [9] to enhance conventional authentication mechanisms for providing secure access to resources in cloud environments. The proposed system combines between recognition-based technique and DAS (Draw-A-Secret) method. It provides a grid consists of 3x3 images for the user to choose, and then the user should paint his path over the selected image as a password.

Chang et al. [10] have proposed KDA system (Keystroke Dynamic-based Authentication) for touch-screen devices. It enlarges the password space-size and encourages the KDA usage in mobile devices. Moreover, authors have explored a pressure feature, which is easy to use in handheld devices, and applied it to the proposed scheme. The experimental results show that the proposed scheme reduces shoulder surfing attacks even if the password is exposed.

Martin et al. [11] have developed a web-based graphical authentication scheme called ImagePass. It relies on one-time passwords for increasing security without compromising its usability. The authors investigated the perception of users regarding graphical recognition-based schemes used in web environments. They examined whether image content influences the memorability of authentication keys. Moreover, how this frequency of use may affect system usability through mnemonic instructions to improve the recognition rate of graphical passwords.

In [12], the authors suggested an authentication approach to generalize the notion of a textual password for improving security. They have introduced a Graphical Password Authentication System (GPAS), which is similar to PassPoint scheme and it conveys authentication information graphically. Users select and answer a set of questions given by the server during the registration phase. Afterward, the authentication server shows images as a challenge in the authentication process and users must pick the correct image to answer the given question.

A graphical recall-based authentication scheme in [13] involves triple verification layers. The authors improved the security of PassGo scheme by adding secret questions, responses, and background images. Initially, the user has to answer a secret question and then insert a background image behind the grid. After that, the user generates a password by connecting points using a straight line to draw a shape.

A graphical random authentication technique (gRAT) was proposed in [14]. It is a swipe-based scheme, which emphasizes both usability and user authentication simultaneously. The user selects a graphical password from a grid of 3x3 images and then swipes a pattern to the images. In the authentication process, gRAT generates a set of images randomly, where the user has to draw the same pattern in the correct order.

The scheme developed in [15] integrates the usability and security attributes of both Passface (recognition-based) scheme and Pass-Point (recall-based) algorithm to overcome a set of drawbacks. The registration and authentication processes of the proposed scheme are similar to Pass-Face algorithm in which the user chooses decoy images that are displayed on the screen. Then, the alphanumeric characters must be entered in the same sequence as images selected in the first step.

Another hybrid authentication scheme was presented in [16]. The proposed scheme seamlessly combines security features of Pass-Points and Press Touch Code authentication schemes. While the hybrid graphical password in [17] incorporates recognition and recall based schemes. Users select their usernames and text-based passwords in the registration process. Then, objects would be displayed to users to choose their graphical passwords. After that, the chosen objects must be drawn on a touch-screen using a stylus. In the authentication phase, users will include their usernames and textual passwords and apply their graphical password in the same manner as they did in the registration process.

Varshney et al. [18] proposed a hybrid graphical authentication scheme to counter shoulder surfing attacks. It is a combination of text-based and graphical schemes. The user selects an image-password based on the predefined background color, and then he/she has to answer the security question to bypass the authentication phase successfully.

3. Proposed Authentication Scheme

Recognition-based passwords have smaller password spaces compared to alphanumeric passwords that in turn cause security problems that make such type of graphical passwords vulnerable to brute-force attacks.

On the other hand, recall-based passwords improve security by increasing the number of clicks but they become more sophisticated. Therefore, the number of clicks needed to authenticate users may vary in amount according to system requirements.

This paper proposes a hybrid graphical user authentication scheme to overcome the security limitations of both recognition-based and recall-based techniques.

The proposed scheme is a multi-factor authentication system whereby the user in a short time interval has to pass successfully three challenges that depend on each other for authentication. First, a grid of decoy images is displayed in random order and the user must pick up the correct image. Then, image-related questions appear and prompt the user to choose the correct secret question of the selected image identified during the registration process. Finally, the user has to click on the right hotspot over the particular image to answer the question.

The time duration for displaying the image is a critical factor in the authentication system. The long display period helps the user to apply the authentication procedures easily. However, the authentication process will take a long time, which gives the attacker enough time to guess the password.

The hybrid authentication system consists of two phases; registration and authentication. In the registration process, the user must register with an authentication system to obtain cloud services, while the authentication procedure verifies the identity of the user every time he/she seeks to access cloud computing services or resources.

3.1 Registration Phase

Figure 1 shows the systematic construction of the registration phase. Steps that comprised the round are enclosed within a dotted rectangle.

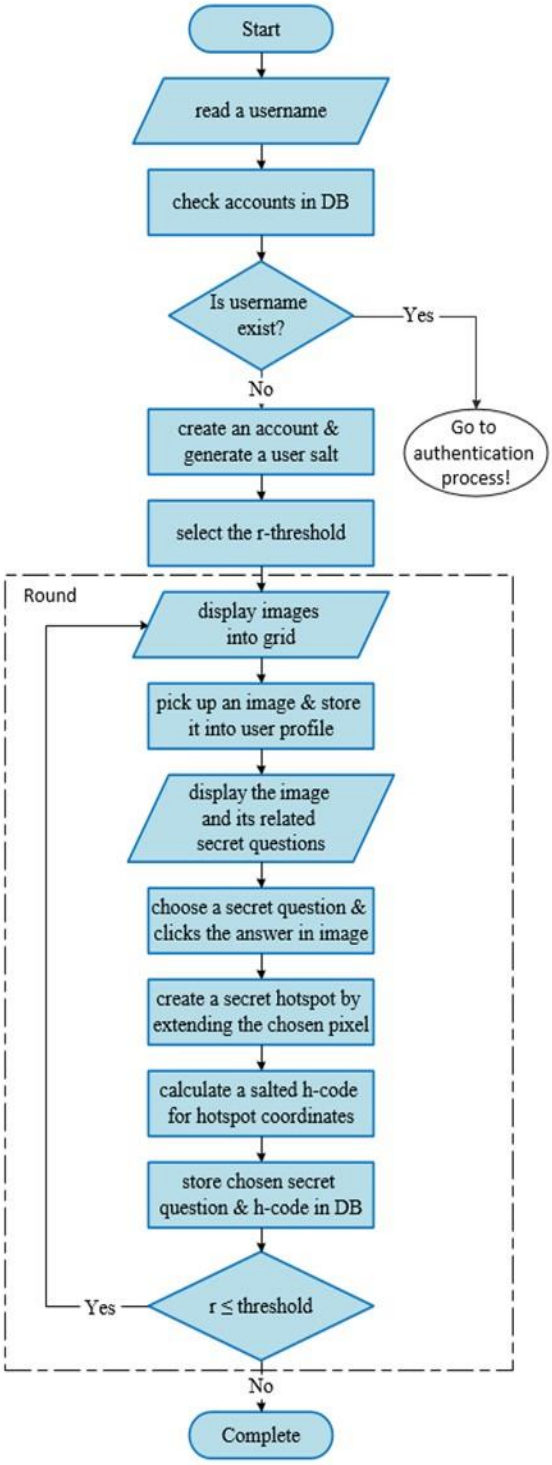

Figure 1. Registration steps

Initially, a new user is required to create an account and register a unique username in the cloud system. At this moment, a random salt string is generated and stored in the user profile for later use in the hashing process.

The registration process consists of three easy steps. In the first step, the grid of images is displayed to the user. The user has to choose one image from those shown in the grid. The proposed scheme distributes images into classes each contains different objects such as colors, animals, cities, and so forth that users can use for creating their graphical passwords. Second, the authentication server shows the selected image in the previous step with three related secret questions. The user has to choose one secret question, which helps him/her to remember the secret hotspot over the image. Finally, the user clicks on any area of the image to answer the question.

The position taped by the user is almost extended to cover a group of nearby pixels to be identified as a secret hotspot. If the size of the specified area is too small, the security level will be high, but the rejection rate will also be high. While if this area is very large, it will be easy for attackers to guess the clickable area.

To provide confidentiality of the selected area, coordinates of the secret hotspot be combined with the random salt string recorded in the user profile and then hashed using any hashing algorithm such as SHA256. Afterward, the hashed value is stored in the database of cloud computing. The selected image itself is not private and might be used by other users but the hotspot selected by the user on the image is secret. Furthermore, the secret question helps the user to remember and find the secret hotspot area in the image during the authentication process.

3.2 Authentication Phase

In this phase, the same registration steps used to create a graphical password are repeated to verify the user identity. First, the user should enter his/her registered username to get the first authentication challenge. The user is required to pass all three challenges correctly to login to the system. If anyone of given challenges in any of the three steps is failed, the account is logged out and the user has to try again. In case the user has failed in the three allowed attempts, the account is blocked.

Figure 2 shows the authentication steps of the proposed scheme. Initially, small images are displayed into a grid. In every round, the image with the lowest weight is shown in the grid with a set of decoy images. Image-weight indicates the number of times users have used the image to access the system. Afterward, the user has to pick and recognize the correct image that was previously identified during the registration phase to bypass the first challenge. Subsequently, the system requires the user to choose the pre-defined secret question related to the password-image as well as click on the correct location in the image to bypass the second and third challenges, respectively.

4. Security and Usability Analysis

The main three security features of the proposed graphical password are decoy images, secret questions, as well as the pre-selected hotspot area inside the selected image. In the authentication process, the user must pass through all these layers successfully to obtain access to the cloud computing system. The security features of proposed scheme are analyzed with regard to different authentication aspects such as password space, entropy of security challenges, and analysis of potential security attacks such as brute-force, guessing, and shoulder surfing attacks.

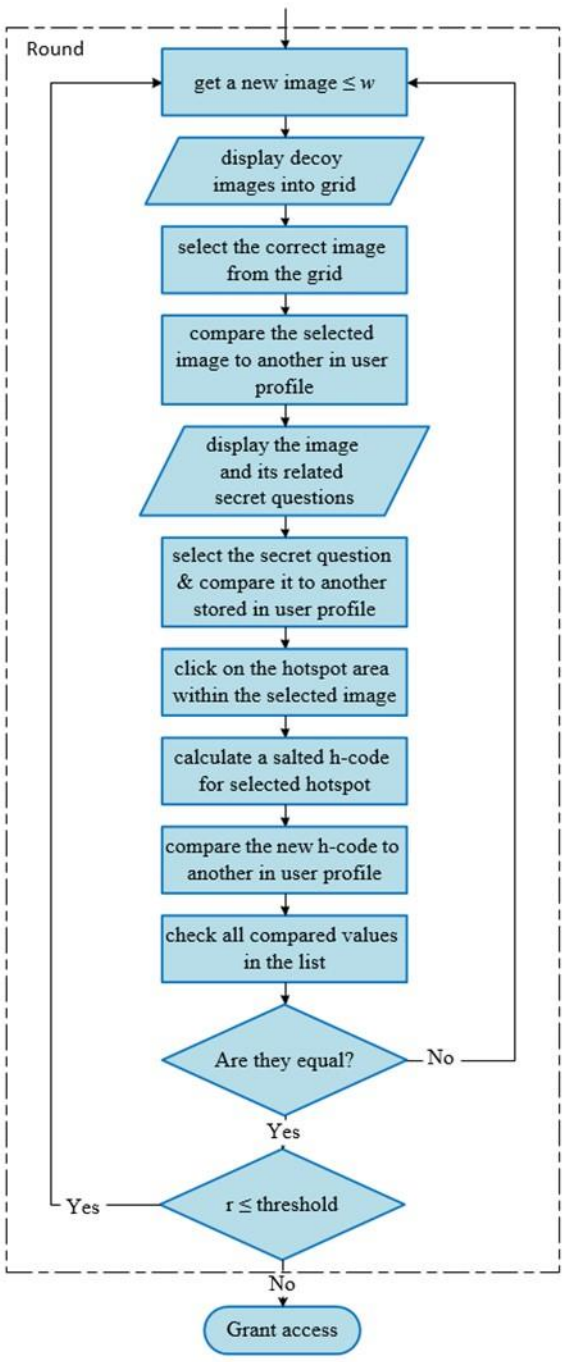

Figure 2. Authentication steps in every round

4.1 Image-based Password Space

Password space is defined as the size of composite keys that can be applied to the authentication system. It computes all possible passwords and provides options for users to choose a password in the authentication scheme.

Password space plays an essential role in the security of the image-based password scheme. Sufficiently increasing the password space can effectively counter brute force attacks. Conversely, brute force attacks lead to serious security problems, if password space is limited. On this basis, the password space must be taken into consideration when designing a graphical password scheme. The password space formulas for three stages of the proposed authentication scheme will be presented in this section. In the first stage, the user has to select the predefined image among a set of images distributed into the given grid. Assume N is the available images in the database, and n is the number of selected images by the user. The password space for the selection stage (S) is calculated using (1).

$$S = \sum_{i=1}^{n} N^n \quad (1)$$

The formula of password space for given questions in the scheme is presented in (2).

$$Q = \sum_{i=1}^{q} T^q \quad (2)$$

Where, q – the number of given questions per round, T – the total number of questions in the scheme.

In the last stage, the user has to choose the correct point as a challenge in the selected image. In this case, the user clicks on the concrete pixel within the image to respond to the challenge. To compute the password space of this stage, the resolution of the image (R) and its size (Z) have been considered as follows, where c – the number of clicks per round.

$$A = \sum_{i=1}^{c} \left(\frac{R}{Z} \right)^c \quad (3)$$

Finally, the password space of the whole scheme can be calculated by combining (1), (2), and (3) in (4); where, r – the number of rounds in the scheme.

$$P_s = \sum_{i=1}^{r} \left(S \times Q \times A \right)^r \quad (4)$$

As seen in (4), as long as the number of rounds is high, the password space will be high as well.

4.2 Entropy of Security Challenges

Password entropy is mostly used to assess the strength of a password and its effectiveness against brute-force or guessing attacks. It estimates how many trials an attacker would need to guess it probably. In this context, an analogous measure is certainly desirable for graphical passwords. The entropy formula presented in [19] has been used to estimate the maximum possible uncertainty of authentication choices.

In our case, according to the hybrid authentication scheme, the uncertainty of choices are the selection of image from a given grid, the choice of the related secret question, and click on the correct area within the selected image. Each choice is conditioned on the previous selection.

The entropy of selecting an image from a grid is equal,

$$H(G) = -\sum_{i=1}^{n} p(g_i) \log_2 p(g_i) \quad (5)$$

where, G – the group of images that are displayed in the grid, n – the number of selected images in the group G, and $p(g_i)$ – the probability of selecting image i in G.

The entropy of selecting a proper question in the list is calculated as follows:

$$H(L|G) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(g_i, l_j) \log_2 p(l_j | g_i) \quad (6)$$

where, L – the list of questions stored in the DB, $P(l_j)$ – the probability of selecting a proper question from L. As shown in (6), the selection of a question is conditioned on the correct selection of the small image in the first step.

Finally, the entropy of selecting the correct point in the image, which conditioned on the previous choices is equal,

$$H(L|GL) = -\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{r} p(g_i, l_j, c_k)\log_2 p(c_k|g_i, l_j) \quad (7)$$

where, C – the total of click-points in every image, $P(c_k)$ – the probability of finding the correct position in the image. The total entropy for the proposed graphical password is calculated as follows,

$$H(GLC) = H(G) + H(L|G) + H(C|GL) \quad (8)$$

where E is a password entropy in bits, N – the available number of challenges, and l – the length of a graphical password.

High password entropy makes the graphical password secure and resisted against potential password attacks.

4.3 Graphical Password Attacks

In this section, the security of the proposed scheme is analyzed with respect to its resistance against most potential attacks that may threaten graphical passwords namely brute force password guessing attacks and shoulder surfing attacks.

4.3.1 Brute-Force Password Guessing Attacks

A brute-force attack discovers a password by applying exhaustive-search, which involves all possible variations until the correct password is found. Theoretically, the strategy of this attack relies on discovering passwords with sufficient computing power and an acceptable time. For this reason, this attack becomes infeasible when the password space is large enough. In this context, increasing the number of decoy images in the grid in addition to the number of potential clicks on the specified image help to thwart such type of password guessing attacks. Moreover, salt included when computing the hash code of image-based fingerprint makes guessing attacks more difficult even though if two users who happen to have the same image clicks will have different fingerprints.

Furthermore, the proposed scheme enforces the user to register three attempts with separate graphical passwords to reduce the probability of brute-force attacks without affecting the usability of the system and the ability of users to remember passwords. A maximum of three experiments per user has been allocated in order to restrict the number of trails by brute-force attackers. If after three attempts the user fails to log in, the account will be banned. This blocking feature can also decrease guessing attacks.

4.3.2 Shoulder Surfing Attack

Shoulder surfing refers to a person who directly observes the victim's device to capture his/her password. Due to the use of visual interfaces on mobile devices, shoulder surfing attack has increased as a serious security risk for graphical passwords. Most current graphical authentication systems are vulnerable to shoulder surfing attacks.

The proposed scheme offers some features to improve security and deter shoulder surfing attacks. The decoy images inside the grid and related secret questions are randomly distributed in different places every time the user creates a password or even uses his/her password to log into the system. In the same context, displaying the image with the least weight on the screen prevents the same image from being used repeatedly as a password during the authentication process. Moreover, the scheme forces the user to log into the system in a short time so that it is difficult for the intruder to notice along with the correct clicks.

4.4 Usability Analysis

The proposed authentication method operates autonomously over any cloud-computing platform using web resources. This method is convenient for users who do not wish to store or share their sensitive personal data on external devices or cloud servers that they have no control over. It also enables the user to use any device (even if it is not trusted) for connection to the cloud computing without worrying that their confidential data will be revealed in case the device was compromised by a third party. Furthermore, the proposed scheme does not include any complicated mechanism where users can easily remember their password through the logical relationship between authentication stages.

5. Experimental Study

Since it is difficult to estimate the security of image-based passwords, the user study has been applied to assess the efficiency of the proposed authentication scheme by evaluating memorability and effectiveness metrics. In the experiment, 74 participants were recruited to participate in this study, 12 of whom were excluded for the following reasons:

1. They registered their graphical password but did not confirm it by logging into the system.
2. They tried to log in after registration but failed in three attempts, which means that they did not carefully notice the password they created during the registration process.

The remaining 62 participants (46 male and 16 female) are from various disciplines and work in different fields. Some of them are students, engineers, doctors, teachers, IT employers and experts, and faculty as shown in Figure 3.

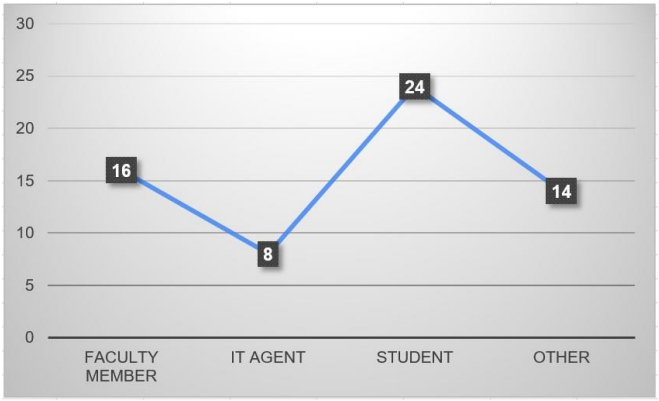

Figure 3. Disciplines of participants in the study

All participants were able to access the system online remotely at any time and from different locations. Participants could freely choose the device they prefer to use in the experiment, either smartphone or desktop. Thirty-six participants used their tablets and mobile devices, while twenty-two participants only used desktop devices (personal computers or laptops).

5.1 Experiment Setup

In this experiment, the proposed authentication scheme was developed using Python programming language (Flask web framework) and then uploaded to a web server.

We have collected 45 multi-object images classified into three classes. Each class contains 15 images distributed randomly over a 3x5 layout as shown in Figure 4.

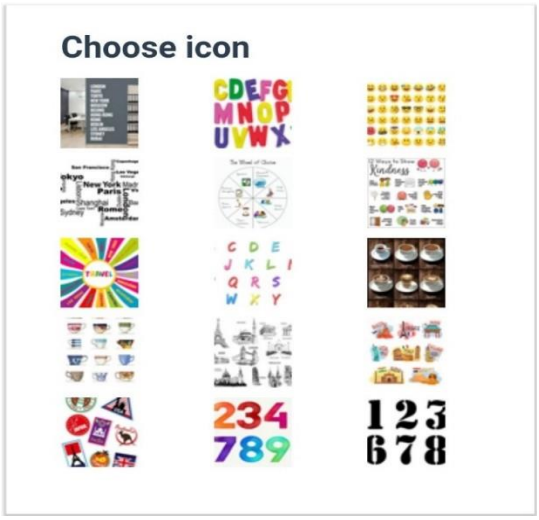

Figure 4. Grid of decoy images

All images were edited with Adobe Photoshop software and then loaded into MySQL database server. Each image is stored twice in small and large formats. The small one appears in the grid, while the other one is the same large image for use by the user as an image-password. Large image size ranges between 280 x 480 pixels to 480 x 480 pixels for portrait images and 480 x 280 pixels to 480 x 480 for landscape images. Besides, we have prepared 20 questions related to the objects included in the available images. Every image has been associated with three different questions.

Figure 5 shows three secret questions related to the selected image. The use of secret questions enables users to click different points in the same image that contains many objects.

Figure 5 shows three secret questions related to the selected image. The use of secret questions enables users to click different points in the same image that contains many objects.

The histogram in Figure 6 shows click-points that some users have made on the same image. In general, the spread of choices appears as a result of the different interests of the users on the one hand and the diversity of the answers that depend on the secret questions that were chosen in advance.

5.2 Procedure

Initially, the participants were asked to watch a tutorial video to ensure that they had the necessary knowledge about how the system works. Thereafter, they are required to register and log in to the system to confirm their graphical password. In the registration phase, participants were required to register three various graphical passwords. Furthermore, the participants were given unlimited trials during the first login process to familiarize themselves with the system. During the authentication after choosing the correct image and secret question, the user must click within an area of 30x30 pixels around the specified point in the corresponding image. To assess the memorability and usability, 40 participants were asked to log in again to the system one-week later. In this session, they were given a maximum of three attempts to login successfully otherwise the account will be blocked, and the sign-in process will be marked as failed. Besides, the effectiveness measure is also analyzed to measure the usability of the scheme and therefore easy to use.

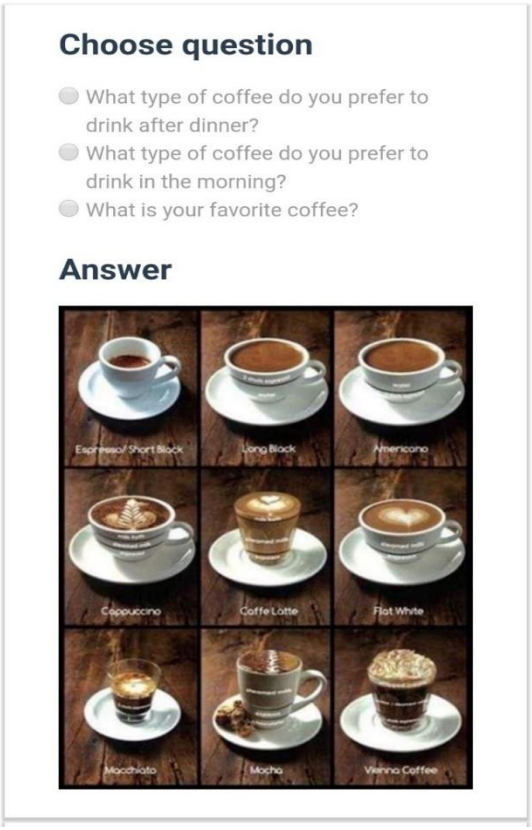

Figure 5. Question-based selected image

The effectiveness is assessed by monitoring the time spent by users to register and log in to the system. We measured the registration time and login time for the first and second sessions. Furthermore, the success rate is measured to evaluate the efficiency of the scheme in terms of record the number of success logins in the second session. The success rate shows users' ability to remember their graphical password. To this end, participants are invited to respond to a questionnaire after registrations and logins to acquire their feedback on the proposed authentication system. Finally, all results and observations were recorded.

Figure 6. Histogram of the click-points

5.3 Results and Discussions

This section presents and discusses the experiment findings when testing the efficiency and effectiveness of the proposed authentication scheme to assess the usability and ease of use. Since this developed authentication scheme combines three different methods to authenticate the identity of the user, we were not able to compare the results obtained with other authentication techniques that may rely on one or two-hybrid authentication methods as a maximum.

5.3.1 Effectiveness Evaluation

Table 1 shows the average time spent by all participants (62 persons) in the first session in registration and verifying processes, as well as the average time spent in the second session in which 40 persons (randomly selected) participated from among those who participated in the first time.

Table 1. Average registration- and login durations

Reg. time	Login time	
	First session	Second session
85s	25.5s	28.4s

The proposed scheme spends less time on registration and authentication processes. We can notice that the average registration time spent by participants in registering three different graphic passwords is 85 seconds. On the other hand, the convergence of the time spent by users during the verification process in the first session with time in the second session (after a week) shows the ease of using the system and remembering the graphical password. Furthermore, it indicates that the usability of the developed scheme can be improved over time with repetition of use.

5.3.2 Efficiency Evaluation

The success rate of the aggregated login attempts in the second session was measured to assess the ability of users to remember their passwords generated before. Figure 7 shows the percentage of attempts that participants successfully logged in to the system.

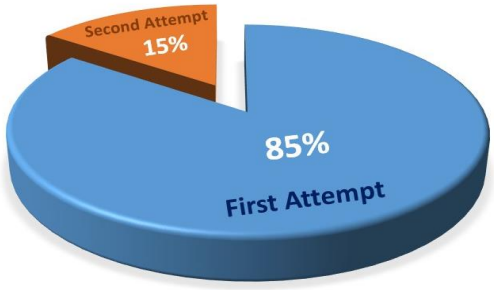

Figure 7. Success rate of the login attempts

As shown in Figure 7, 85% of the participants were able to log in successfully for their first time, which proves that this developed scheme is easy to remember and easy to use.

5.3.3 User Satisfaction

At the end of the experiment, an online survey has been conducted to evaluate the effectiveness of the method and reflect user satisfaction.

The survey mainly consists of three questions that are ranked on a 5-point Likert scale: Strongly agree, Agree, Neutral, Disagree, and Strongly disagree. The survey questions are as follows;

1. Do you think the registration procedures are easy to follow?
2. Do you think the registration phase was boring?
3. Could you easily remember your graphical password during the login process?

The questionnaire results that are acquired from the respondents are plotted in Figures 8, 9, and 10.

In particular, Figure 8 shows the participants' satisfaction with the procedures followed during the registration process.

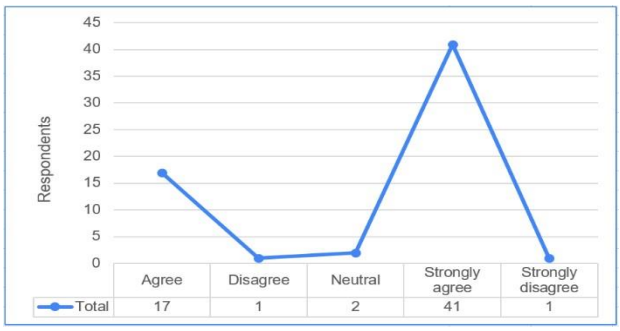

Figure 8. Responses to the first question

The results indicate that most of the respondents (94%) found the registration procedures are easy and uncomplicated even though they were required to register three different graphic passwords.

Findings regarding the answer to the second question of whether the registration process is boring for the participants or not. As shown in Figure 9, 89% of the participants thought that it was not boring.

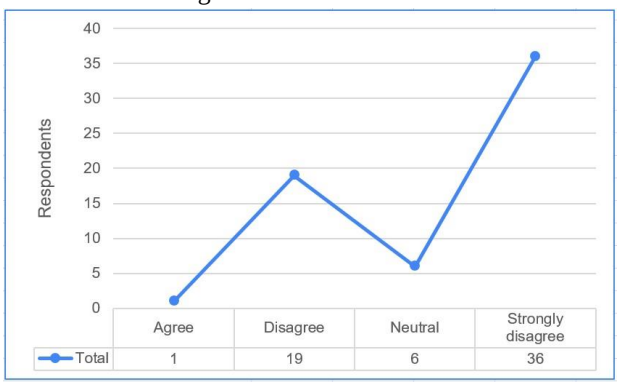

Figure 9. Responses to the second question

Figure 10 shows the result of the third question. It illustrates the ability of participants to remember the graphical password during the login process. 63% and 29% of the participants strongly agreed and agreed, respectively, which means that it was easy for them to remember the password. These findings confirm that the authentication scheme used is generally easy to use.

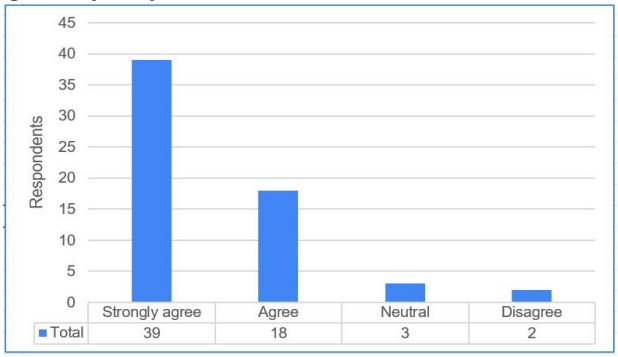

Figure 10. Responses to the third question

6. Conclusions

This paper presented a hybrid graphical-based user authentication scheme for portable cloud computing environments. The proposed scheme consists of registration and authentication phases. In the registration phase, the user needs to register with the authentication server, while the authentication phase verifies the identity of the user before accessing cloud services and resources. The authentication scheme can be secured from any potential attacks since there are no sensitive details about the chosen graphical password have been stored on the cloud computing sites.

The experimental study and survey have been conducted to investigate the user satisfaction of the proposed authentication scheme concerning the performance and usability aspects. In the evaluation of the password usability, the login duration and the success rate have been measured. Results showed that the proposed authentication scheme is secure, reliable, and easy to use.

7. Acknowledgement

The authors gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the material support for this research under the project number: 5247-coc-2018-1-14-S during the academic year 1439 AH/2018 AD.

References

[1] F. Towhidi, M. Masrom, "A survey on recognition-based graphical user authentication algorithms", International Journal of Computer Science and Information Security. Vol. 6, No. 2, pp. 119-127, 2009.

[2] S. Xiaoyuan, Z. Ying, G. Scott, "Graphical passwords: a survey", 21st Annual Computer Security Applications Conference *(ACSAC'05)*, Tucson, AZ, pp. 463-472, 2005

[3] W. Hu, X. Wu, G. Wei, "The Security Analysis of Graphical Passwords," International Conference on Communications and Intelligence Information Security, Nanning, pp. 200-203, 2010.

[4] G. Haichang, J. Wei, Y. Fei, M. Licheng. "A Survey on the Use of Graphical Passwords in Security", Journal of Software, Vol. 8, No. 7, pp. 1678-1698, 2013.

[5] K. Benzidane, S. Khoudali, L. Fetjah, S. J. Andaloussi and A. Sekkaki, "Application-Based Authentication on an Inter-VM Traffic in a Cloud Environment", International Journal of Communication Networks and Information Security. Vol. 11, No. 1, pp. 148-166, 2019.

[6] K. Renaud, E. Olsen. "DynaHand: Observation-Resistant Recognition-Based Web Authentication", IEEE Technology and Society Magazine, Vol. 26, No. 2, pp. 22-31, 2007.

[7] Z. Zheng, X. Liu, L. Yin, Z. Liu, "A Hybrid Password Authentication Scheme Based on Shape and Text", Journal of Computers, Vol. 5, No. 5, pp. 765-772, 2010.

[8] S. M. Gurav, L. S. Gawade, P. K. Rane, N. R. Khochare, "Graphical Password Authentication: Cloud securing scheme", International Conference on Electronic Systems, Signal Processing, and Computing Technologies, Nagpur, pp. 479-483, 2014.

[9] G. Ming-Huang, L. Horng-Twu, H. Li-Lin, Y. Chih-Ta, "Authentication Using Graphical Password in Cloud", 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, pp. 177-181, 2012

[10] T. Y. Chang, C. J. Tsai, J. H. Lin. "A Graphical-Based Password Keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices". Journal of Systems and Software, vol. 85, no. 5, pp.1157-1165, 2012.

[11] M. Mihajlov, J. Borka. "On designing usable and secure recognition-based graphical authentication mechanisms", Interacting with Computers, Vol. 23, pp. 582–593, 2011.

[12] N. A. Pogale, G. R. Deepak, "A Secure Authentication Using Graphical Password Authentication System: GPAS", International Journal of Advanced Research in Computer Science, Vol. 4, No. 6, pp. 270-273, 2013.

[13] B. Togookhuu, J. Zhang, "New Graphical Password Scheme Containing Questions-Background-Pattern and Implementation". Procedia Computer Science, Vol. 107, pp. 148-156, 2017.

[14] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, K. A. Awan. "g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices," IEEE Transactions on Consumer Electronics, Vol. 65, No. 2, pp. 215-223, 2019.

[15] T. Zangooei, M. Mansoori, I. Welch. "A Hybrid Recognition and Recall Based Approach in Graphical Passwords", 24th Australian Computer-Human Interaction Conference, Australia, pp. 665-673, 2012.

[16] S. Azad, N. E. A. C. Nordin, N. N. A. Rasul, M. Mahmud, K. Z. Zamli. "A Secure Hybrid Authentication Scheme Using Pass-points and Press Touch Code," IEEE Access, Vol. 7, pp. 166043-166053, 2019.

[17] W. Z. Khan, M. Y. Aalsalem, Y. Xiang. "A Graphical Password-Based System for Small Mobile Devices", International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, pp. 145-154, 2011.

[18] S. Varshney, M.S. Umar, A. Nazir. "A Secure Shoulder Surfing Resistant Hybrid Graphical User Authentication Scheme", Cybernetics, Cognition, and Machine Learning Applications. Algorithms for Intelligent Systems. Springer, Singapore, pp. 79-87, 2020.

[19] S. Rass, D. Schuller, C. Kollmitzer, "Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication", International Conference on Communications and Multimedia Security, Berlin, Heidelberg, pp 166-177, 2010.