International Journal of Engineering & Technology, 7 (4.19) (2018) 193-198

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Authentication Mechanisms for Mobile Learning Applications: a Usability Study

Kang Hean Yong[1], Norliza Katuk[2*], Nur Haryani Zakaria[2]

[1]Tuanku Abdul Rahman University College, 77, Lorong Lembah Permai Tiga, Tanjung Tokong, 11200 Tanjung Bungah, Pulau Pinang.
[2]School of Computing, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia.
**Corresponding Author Email: [2]k.norliza@uum.edu.my*

Abstract

Authentication is a security component that maintains user access to applications. It has been the primary reason for users to create usernames and passwords before they can use applications. In creating usernames and passwords; users are required to fill in their personal information in which it is a time-consuming process. Additionally, it also increases the number of usernames and passwords that users need to remember which leads to password fatigue. Social login is a way to address this problem. With the benefits that social login could offer, this study aims to study the usability of social login for mobile learning. Further, the user's preference towards authentication mechanisms used for mobile learning applications was identified. An experimental study was conducted using a mobile learning application named LANGKAWI ISLANDS. Forty participants participated in this study on a voluntary basis and used the traditional and social login on LANGKAWI ISLANDS. The time taken by the participants to sign up the application using both mechanisms was recorded. The usability of the authentication mechanisms was evaluated using a self-report questionnaire. Then, the participants stated their preference for the authentication mechanisms. The results suggest that the social login is more usable than the traditional authentication mechanism. Further, the users' signup process for LANGKAWI ISLANDS is much faster using social login and has been the primary users' preference for mobile learning authentication mechanism.

Keywords: *User authentication; social network; social network login; social login; user credentials.*

1. Introduction

Today's smartphones and tablets have enabled users to access various applications on a mobile basis without having to use a desktop computer as before. These applications include mobile banking, mobile payment, mobile shopping and mobile learning [1]; just to name a few. In the context of education, mobile learning encourages independent and collaborative experience among learners [2]. Mobile phone technology has been combined with learning theories to give students more flexibility and engaging learning experience. It is essential to ensure that learning is appropriately designed so that it can transform teachers' and students' mindset towards a more productive learning environment to achieve effective integration [3]. Further, a successful learning process is highly depending on the learning environment's service quality and stakeholder satisfaction [4]. The process of delivering learning content to students through smartphones involving the technical design of mobile applications including interface, navigation, accessibility, and personality is an example of service quality and satisfaction.

Many applications (either web or mobile) enforce users to create a credential (usually a username and password) for authentication and personalization. Apart from the credentials, the traditional authentication mechanism requires users to provide their personal detail such as name, gender, and age during the registration or signup process which is a time-consuming task for many people. It also increases the number of credentials that users have to remember which may lead to password fatigue [5]. Developers shift from the traditional authentication mechanism to social login; a mechanism to log in to a particular application using social network credentials to improve this issue [6]. Currently, there is a growing interest among developers to use social login such as LinkedIn, Google+, Facebook or Twitter for authentication mechanism of their applications. Social login is simple, and it provides a useful mean for user authentication without having to create an additional profile [7, 8].

Social login has been found as a standard feature of social commerce websites [9]. Recently, there is a growing interest among mobile learning application providers on the use of social login for their user authentication. Social login has been used in popular mobile learning applications such as Coursera and Course Guru. Looking at the benefits that social login could offer, this study aims to evaluate the usability of authentication mechanisms for mobile learning applications from three perspectives namely usefulness, ease of use and satisfaction. Further, the study intends to understand learners' preference towards these authentication mechanisms. This article describes the detail information about this study. First, the following section explains the concept of social login and its application in mobile learning environment briefly. Then, Section 3 describes the method, hypotheses, the materials, the participants and the procedure for conducting the experimental study.

The results obtained from the experimental study is presented and discussed in Section 4. Finally, the limitations of the study and the future works are explained in Section 5.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Mobile Learning Using Social Login Authentication

Authentication mechanisms are initially needed in critical systems to validate that users are legitimate and have access right to the content requested from a particular system. However, nowadays, as the technology grows exponentially with various innovations in systems are being introduced, authentication mechanisms work beyond that function. For example, within the web and mobile applications, authentication mechanisms also aim at providing users with adaptive content. Hence, it will increase the user experience in several ways when they use the applications. However, the increasing number of applications that require users to create username and password has led to password fatigue [10], an exhausted feeling that users experience when they have to remember too many usernames and passwords every day to login to many systems and applications. Due to this situation, researchers and developers have started on working towards reducing the number of login credentials that users have to hold at one time. An authentication mechanism through social login is among one of the feasible solutions aims at accommodating a user demand for a reduction in login credentials [11]. New users who need to use applications will sign in with their existing username and password for social networking services such as Facebook, Twitter, and Google+ [12],[13].



Fig. 1: Example of social login buttons

As described earlier, application providers use social login to allow users to access to their applications by using the users' existing social network credentials [6]. The use of social network credentials will reduce password fatigue and eliminate the registration process [8] where users do not have to key in their personal information anymore. It eliminates the need for the users to refill a form, choose a username and secure password and simplifies the registration of a new user to an application. Ultimately, it simplifies the whole registration process which shortens the time to access the application for the first time, and straight away direct the users to the content of the application. By signing in using the social network username and password, users are allowing mobile applications to access their public profile such as demographic data, email address and friends as well as to request extended profile properties including the history of users' likes or recorded web activities. This profile information will be useful to the application providers for creating personalized content for individual users. From the perspective of application providers, social logins allow applications and services easier and faster to develop and deploy [14]. It does not require the providers to create a specific database for user credentials and does not need to prepare a separate form for user's registration. Further, users' profile information can be derived from the social network providers and can be customized to the requirements of the intended applications.

Although social logins address password fatigue successfully, users and developers are concerned on the security aspects of the authentication mechanism as many parties are involved and how the credentials are being protected from attacks and threats is not transparent. Social login might not be suitable for a particular domain of application such as mobile banking; however, a less critical domain such as mobile learning could benefit from it. There is an increased interest among mobile learning application providers on the integration of social login on their application. For example, Coursera and CourseGuru, among a prevalent web and mobile learning providers embed social login (Facebook and Google+) to their applications as shown in Figure 2 and 3 respectively.

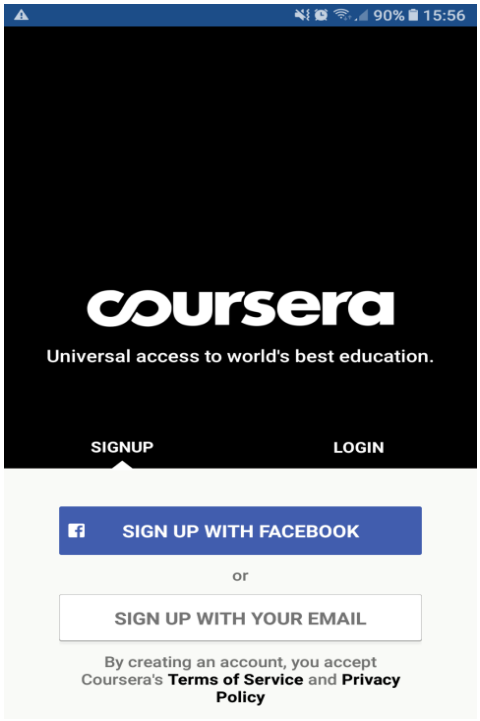


Fig. 2: Facebook login button in Coursera app

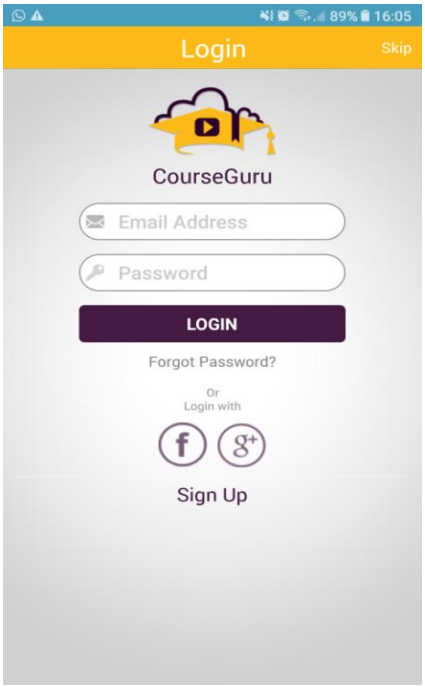


Fig. 3: Facebook and Google+ login buttons in Course Guru app

The mobile learning environment should be adaptive to individual learners' needs to achieve more effective and engaging learning. Adaptive mobile learning applications could employ social logins to extract information about the learners [15]. It is inconvenient to register a user account one by one manually. Many of the mobile applications today support social login. For mobile learning applications designed for institutions, it is a tedious job to create user credentials for every learner in the institution. Managing and

communicating the temporary credentials are also tedious if it involves many users. Sometimes students hardly used the credentials created by the institutions, which consequently hinder mobile learning. By using social login, learners just need to sign in the mobile learning applications with their social network credentials and the server will automatically pull the data from the corresponding authentication service providers (e.g., Facebook). As a result, the application providers can avoid running the signup process and instead directly run the application to trigger the social login interface. Further, social logins are more familiar to the learners and make it more convenient for them to participate in the mobile learning, as they only need to memorize and maintain single username and password [16]. End users choose social login because of the convenience of the overall authentication process. Social network credential provided by the primary social network providers (e.g., Facebook, Twitter, Google+) has gone beyond the service that focused on authentication and identity management solutions. It also provides useful user profile information. The user profile can be customized to create personalized content for individual learners [17],[18] of mobile learning applications. Personalized learning content is essential to assist learners to understand the topic of learning better, and provide an engaging learning environment.

Research by Egelman [19] shows that although the users of social login understand the implications of privacy, the majority of them still choose to use social login function because of convenience. Convenience in this context is a component of usability where mobile applications should be easy to use to achieve the users' objective [20]. As the integration of social login in a mobile learning application is limited in terms of its application; hence, there is a need to study how users perceive the usability of the authentication mechanisms in the mobile learning environment.

3. Experimental study

3.1. Method and Hypotheses

This study was carried out following the within-subject design experimental study. The independent variable was the types of authentication mechanism (i.e., traditional and social login) while the dependent variables were usability of the authentication mechanism; signup time (in seconds), and user's preference. The following three hypotheses were formulated for this study:

HA: There is a difference concerning the usability of LANGKAWI ISLANDS using social login and the traditional authentication mechanisms;

HB: There is a difference concerning time taken for the participants to sign up LANGKAWI ISLANDS using social login and the traditional authentication mechanisms; and

HC: There is a difference concerning users' preference of social login and traditional authentication mechanisms for LANGKAWI ISLANDS.

3.2. Materials

The experimental study was conducted using two main instruments that include a mobile learning application namely LANGKAWI ISLANDS and a questionnaire asking on the participants' background information (i.e., age and gender), the usability components (i.e., usefulness, ease-of-use, and satisfaction) and their preference of the authentication mechanisms. Usefulness, Satisfaction, and Ease of use (USE) Questionnaire [21] was adapted in this study. It contained 26 items measured in a seven-point Likert scale where one represents strongly disagree, and seven represents strongly agree. USE Questionnaire has also been used as an instrument for measuring usability of computer systems in other studies such as in Mahmoud and Hassan [22], Sabri and Hussain [23], Hussain et al. [24], and Razak et al. [25].

LANGKAWI ISLANDS is a mobile learning application that provided the learners with the history of Langkawi Islands in Malaysia. The mobile learning application was developed using Eclipse integrated development environment (IDE). Android software development kit (SDK) and Facebook SDK were imported into the IDE. OAuth 2.0 was the authorization protocol for integrating the Facebook login into LANGKAWI ISLANDS for representing the social login authentication mechanism. Adobe Illustrator CS5 was used as the graphics editing tool. The prototype runs on mobile operating system Android 4.3 Jelly Bean for the experimental study. Figure 4 shows the home interface of LANGKAWI ISLANDS, and one example of the learning interface is visualized in Figure 5.



Fig. 4: The home interface for LANGKAWI ISLANDS

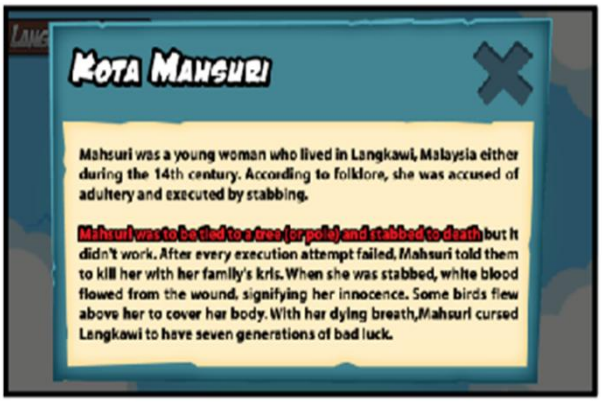


Fig. 5: The example of learning interface in LANGKAWI ISLANDS

LANGKAWI ISLANDS mobile learning application was developed in two versions to demonstrate the social and traditional logins as shown in Figure 6. The traditional login requires the participants to sign up for the first time by creating a username, and password as shown in Figure 7. The social login used the Facebook login button to represent the social login as in Figure 8. Figure 9 shows an example of the interface when a user has successfully signed in using his/her Facebook credential. Table 1 compares the components of the two authentication mechanisms including the registration process, usernames and passwords and login features in LANGKAWI ISLANDS.



Fig. 6: The login interface of LANGKAWI ISLANDS

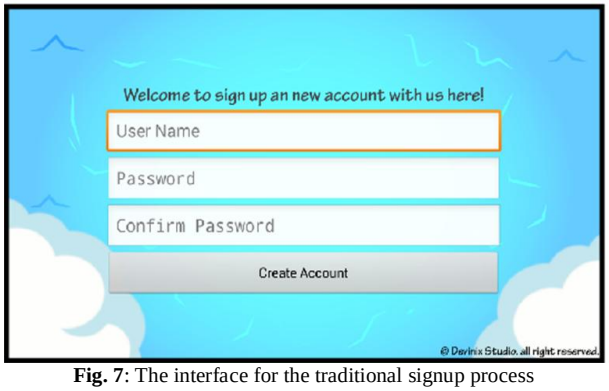


Fig. 7: The interface for the traditional signup process

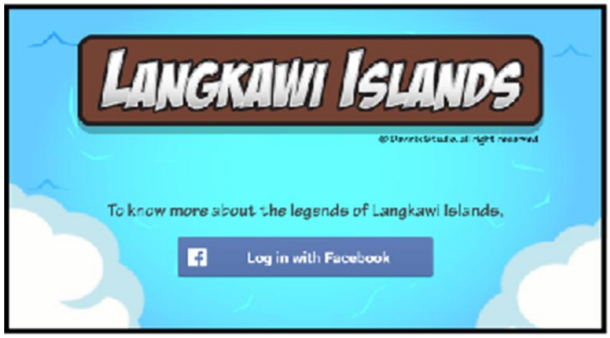


Fig. 8: The interface for the social login

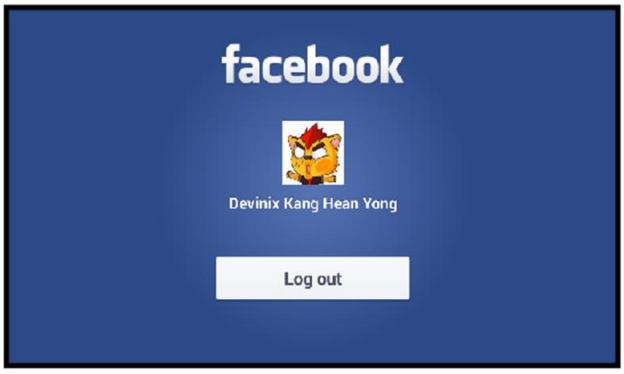


Fig. 9: The interface of a successful login using social login

Table 1: The features of social and traditional logins

Components	Social Login	Traditional Login
Registration process	No. Social network accounts for the evaluation purpose has been created and active in a mobile device.	Manually. Users were required to create a user account by typing in user profile information.
New username and password required	No. Users used the existing social network account username and password.	Yes. Users need to remember the new username and password created.
Login feature	Yes. Users need to click the login button provided on interface and auto login without providing username and password.	Yes. Users were required to supply username and password each time login to the system after logout.

3.3. Participants and Procedure

A group of 40 students (i.e., twenty-two males and eighteen females) from Tunku Abdul Rahman College University (TARUC) aged between nineteen and twenty-four years old participated in this experiment on a voluntary basis. The participants were assigned into two groups at random. Group A consists of nine males and eleven females while group B consists of thirteen males and seven females. The participants in Group A worked with traditional login followed by social login, while the participants in Group B used the reversed sequence of the interfaces. Table 2 shows the procedure for conducting the experiment. During the experiment session, the time spent by the participants to complete the signup process was recorded in second(s) by the experimenter.

Table 2: The procedure for conducting the experiment

STEPS	TASK	
	GROUP 1	GROUP 2
Step 1:	The participant was required to provide demographic and background information.	
Step 2:	The participant was required to execute the test scenarios for traditional login.	The participant was required to execute the test scenarios for social login.
Step 3:	The participant answered post-task questionnaire for traditional login.	The participant answered post-task questionnaire for social login.
Step 4:	The participant answered the post-session questionnaire for traditional login.	The participant answered the post-session questionnaire for social login.
Step 5:	The participant was required to execute the test scenarios for social login.	The participant was required to execute the test scenarios for traditional login.
Step 6:	The participant answered post-task questionnaire for social login.	The participant answered post-task questionnaire for traditional login.
Step 7:	The participant answered the post-session questionnaire for social login.	The participant answered the post-session questionnaire for traditional login.
Step 8:	The participant answered the post-session questionnaire for preferred login facility.	
Step 9:	The participant participated in the post-session interview. (8 participants)	

During the experiment, the participants were divided into two groups, and the two mobile applications with different authentication mechanisms were presented to them in a different order. Therefore, a non-parametric Mann Whitney U test was performed to find out whether the order of presenting different mobile learning applications affect the users' rating on the questionnaire. The results of Mann Whitney U test returned the z values range from -0.285 to -1.097 with a significant level of $p<0.05$. The results suggested that the order of presenting different authentication mechanisms have no effect on the respondents' usability response during the experiment.

4. Results and Discussion

SPSS version 19 was used in data analysis and the statistical tests. A codebook was created to ease the process of data entry. Before starting any test, all the data went through the screening procedure (descriptive statistic) to identify missing values and improve the integrity of data entry. All the test items also suggested high internal consistency where Cronbach's Alpha coefficient values ranging from 0.705–0.903. The data were tested for normal distribution using Kolmogorov-Smirnov tests. The result indicated that not all the dependent variables were normally distributed ($p < 0.05$). Therefore, the data analysis was conducted based on non-parametric tests particularly the Wilcoxon Signed Rank Test and Chi-square goodness-of-fit test.

4.1. The Participants' Background

Most of the participants had high-frequency usage of mobile applications. 90% of them used mobile applications on a daily basis. 37.5% had three or less mobile accounts that need a password, and another 37.5% had four to ten mobile accounts with password. The rest of the participants had quite many mobile accounts (i.e., 21 or more). Within these participants, 82.5% had the experience of using social login to sign up multiple mobile applications.

92.5% of the participants mentioned that they knew about social login.

4.2. The Usability of Authentication Mechanisms for the Mobile Learning Applications

The respondents' usability responses for both authentication mechanisms were analysed by calculating the means, the standard deviations, and the medians as shown in Table 3. The means for three components of usability (i.e., usefulness, ease of use, and satisfaction) for the traditional login are lower than the social login. This has also led to a higher score of the overall usability for social login of the authentication mechanisms.

Table 3: The means, standard deviations and mean ranks (N=40)

Components	Social Login			Traditional Login		
	Mean	S.D.	Med.	Mean	S.D.	Med.
Usefulness	5.74	0.69	5.94	4.27	1.16	4.38
Ease of Use	5.75	0.58	5.73	4.40	1.07	4.45
Satisfaction	5.77	0.89	5.86	4.08	1.15	4.29
Overall Usability	5.75	0.52	5.58	4.25	1.06	4.18

A Wilcoxon Signed Rank test was conducted on the participants' usability responses. The median score on the result showed that the first component of usability (i.e., usefulness) was higher for social login (Md = 5.94) as compared to the traditional login (Md = 4.38). A statistically significant difference also occurs in the usefulness of LANGKAWI ISLANDS application with z=-4.949, p<0.05, and effect size r=0.55. A statistically significant difference also appears in the ease of use of the usability component with z=-5.081, p<0.05, and the effect size r=0.57. The same goes for the satisfaction component where a statistically significant difference with z=-4.976, p<0.05, and effect size r=0.56 was reported. The median score shows that the ease of use was lower for the traditional login (Md = 4.45) as compared to social login (Md = 5.73). On the other hand, the satisfaction of social login score (Md = 5.86) is higher than the traditional login (Md = 4.29). Table 4 shows these values.

Table 4: The statistic values of Wilcoxon Sign Rank Tests (N=40)

Components	Negative Rank		Positive Rank		Tie	Stat. Sig.
	N	Mean Rank	N	Mean Rank		
Usefulness	4	8.88	35	21.27	1	z=-4.949, p<0.05. Sig.
Ease of Use	4	6.50	35	21.54	1	z=-5.081, p<0.05, Sig.
Satisfaction	4	8.38	35	21.33	1	z=-4.976, p<0.05, Sig.
Overall Usability	2	7.25	38	21.20	0	z=-5.316, p<0.05, Sig.

In overall, the test results showed statistically significant differences in usability evaluation with z=-5.316, p<0.05 and effect size r=0.59. The median score of overall usability was improved in the social login (Md = 5.58) as compared to the traditional login (Md = 4.18). Thus, all these results suggested that the social login mechanism had higher usability as compared to the traditional login mechanism concerning its usefulness, ease of use, and satisfaction. Hence, HA is supported.

4.3. The Time for the Sign up Process

As mentioned above, the time taken by the participants during the signup process was recorded. The analysis of the individual participants' time suggested that the mean for the signup time (in seconds) of LANGKAWI ISLANDS using traditional login is 51.65 seconds which is 45.6 seconds more than the social login. Table 5 shows the mean, standard deviation and the median time for both social and traditional logins.

Table 5: The means, standard deviations and mean ranks (N=40)

Components	Social Login			Traditional Login		
	Mean	S.D.	Med.	Mean	S.D.	Med.
Time (in seconds)	6.05	4.50	5.00	51.65	20.16	47.50

A Wilcoxon Signed Ranked test was carried out to compare the time for the signup process, and the results are shown in Table 6. The median time is 47.50 and 5 seconds for the traditional and social logins respectively. The results indicated a statistically significant difference in the signup time where z=-5.512, p<0.05, and effect size r= 0.62. These results revealed that social login in LANGKAWI ISLANDS provided the participants with shorter time to sign up. Based on the result, HB is accepted.

Table 6: The statistic values of Wilcoxon Sign Rank Tests (N=40)

Components	Negative Rank		Positive Rank		Tie	Stat. Sig.
	N	Mean Rank	N	Mean Rank		
Time (in seconds)	40	20.50	0	0	0	z=-5.512, p<0.05. Sig.

4.4. The Users' Preference on Login the Mechanisms

The participants were asked about their preferred authentication mechanism with a question: "In future, if you are going to use this mobile application during your trip, which approach would you use to log in?" Thirty-three participants preferred social login which equals to 82% of the participants. Figure 10 shows the pie chart for the participants' preferred authentication mechanisms.

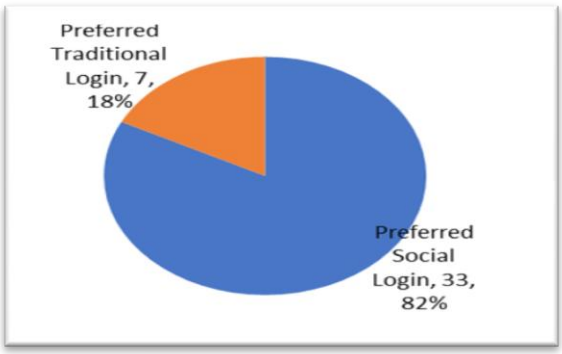


Fig. 10: User's preference on authentication mechanisms

A Chi-square goodness-of-fit test was conducted, and the result revealed that the test statistics is significant with X^2 (1, n=40) = 16.90, p < 0.0005. Therefore, it is suggested that there is a statistically different in the preference of the authentication mechanisms, with fewer people preferring the traditional login (N=7) as compared to social login (N=33). The reasons for their preferences include, 25% of them mentioned that social login was easy to use, 21% of them felt that social login helps to save time in login process, 18% of them emphasized about the convenience of social login, 15% of them felt that social login is faster than traditional login, 3% of them believed that social login helps to reduce the number of passwords to remember, and the remained 18% stated no reason. Among 7 of the participants who preferred traditional login, the majority of them (71%) concerned about the security issue, and 29% of them concerned about the privacy issue. Based on the result, HC is accepted.

5. Conclusion, Limitations and Future Works

This paper presented a study on the usability of authentication mechanisms for mobile learning applications. A mobile learning application named LANGKAWI ISLANDS was used in the experimental study accompanied by the USE questionnaire. Two types of authentication mechanisms namely social login and tradi-

tional login were embedded in LANGKAWI ISLANDS for the usability evaluation. Three hypotheses were formulated and tested in this study covering the usability of the authentication mechanisms; the time taken by the participants for signup process of LANGKAWI ISLANDS, and the preferred authentication mechanisms.

The results of this study confirmed that social login is more usable in terms of usefulness, ease of use, and satisfaction as compared to the traditional login. Further, the results also confirmed that social login is able to speed up the signup process of mobile learning applications; where the average time taken by all participants in registering themselves to the application was shorter than the traditional login. Finally, the results of the study revealed that the social login had been the preferred authentication mechanism for accessing content in mobile learning applications. The findings obtained in this study could provide a general guideline to developers, designers, or instructors of mobile learning applications. They could improve their applications by providing an alternative authentication mechanism for increasing users' convenience.

The outcomes of this study should be used with consideration of limitations in the design of the experimental study. First, it is important to note that the participants were volunteers from a higher learning institution aged between nineteen to twenty-four years old. More generalized results can be obtained if the experiment involves other institutions and different students from various courses.

Further, users with different background and level of academic study could lead to different results. Second, the social network used in the experimental session only involved Facebook with OAuth 2.0 protocol. The steps to complete the OAuth 2.0 connection could be different from other protocols such as OpenID and SAML. Therefore, the result of this study only limited to those social login mechanisms using OAuth 2.0. Further, social login by other social network providers could also lead to different usability results due to the steps in the signup process. Lastly, this experimental study only used one single mobile device for participants to conduct the designed task in the different time frame. The network connection and bandwidth speed were assumed to be same across the different time frame. Besides that, all the participants are first time user of the LANGKAWI ISLANDS which could also affect the results.

Limitations found in this study can be used as the improvement for other similar studies in future. A couple of research idea could be carried out to improve the results of this study. First, participants for such experimental study could be gathered from diverse backgrounds like a mixture of students across different institutions or users from different academic levels. Second, there is an opportunity to study the relationship between security, privacy, and convenience of social login for mobile learning applications.

Acknowledgement

This work was supported by Ministry of Higher Education, Malaysia under the Fundamental Research Grant Scheme (Ref: UUM S/O Code: 13143).

References

[1] H. R. Marriott and M. D. Williams, "Developing a Theoretical Model to Examine Consumer Acceptance Behavior of Mobile Shopping," in Conference on e-Business, e-Services and e-Society, 2016, pp. 261-266.

[2] S. R. Jan, F. Ullah, H. Ali, and F. Khan, "Enhanced and Effective Learning through Mobile Learning an Insight into Students Perception of Mobile Learning at University Level," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN, pp. 2395-1990, 2016.

[3] C. P. Lim and D. Churchill, "Mobile learning," Interactive Learning Environments, vol. 24, pp. 273-276, 2016/02/17 2016.

[4] M. Sarrab, M. Elbasir, and S. Alnaeli, "Towards a quality model of technical aspects for mobile learning services: An empirical investigation," Computers in Human Behavior, vol. 55, pp. 100-112, 2016.

[5] A. Tanti and D. Buhalis, "The influences and consequences of being digitally connected and/or disconnected to travellers," Information Technology & Tourism, vol. 17, pp. 121-141, 2017.

[6] L. K. Moey, N. Katuk, and M. H. Omar, "Social login privacy alert: Does it improve privacy awareness of facebook users?," in Computer Applications & Industrial Electronics (ISCAIE), 2016 IEEE Symposium on, 2016, pp. 95-100.

[7] Y. Madani, J. Bengourram, and M. Erritali, "Social Login and Data Storage in the Big Data File System HDFS," in Proceedings of the International Conference on Compute and Data Analysis, 2017, pp. 91-97.

[8] Y. Madani, J. Bengourram, M. Erritali, B. Hssina, and M. Birjali, "Adaptive e-learning using Genetic Algorithm and Sentiments Analysis in a Big Data System," International Journal of Advanced Computer Science And Applications, vol. 8, pp. 394-403, 2017.

[9] N. B. Ismail and H. M. Dahlan, "Technical features for social commerce website," in Student Project Conference (ICT-ISPC), 2017 6th ICT International, 2017, pp. 1-5.

[10] S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 workshop on New security paradigms, 2010, pp. 61-72.

[11] M. Tsikerdekis, "Real-Time Identity Deception Detection Techniques for Social Media: Optimizations and Challenges," IEEE Internet Computing, 2017.

[12] Y. Li, J. Jiang, and T. Liu, "Inferring User Consumption Preferences from Social Media," IEICE Transaction on Information and Systems, vol. 100, pp. 537-545, 2017.

[13] N. Katuk, H. M. Tahir, N. H. Zakaria, and M. S. Halim, "Can single sign-on improve password management? A focus group study," in Pattern Analysis, Intelligent Security and the Internet of Things, ed: Springer, 2015, pp. 85-93.

[14] S. Iaconesi, "Interface and Data Biopolitics in the Age of Hyperconnectivity. Implications for Design," The Design Journal, vol. 20, pp. S3935-S3944, 2017.

[15] C. Zuo, Q. Zhao, and Z. Lin, "AUTHSCOPE: Towards Automatic Discovery of Vulnerable Authorizations in Online Services," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 799-813.

[16] M. Aristeidou, E. Scanlon, and M. Sharples, "Design Guidelines for Sensor-based Mobile Learning Applications," 2017.

[17] J. Krämer, D. Schnurr, and M. Wohlfarth, "Winners, Losers, and Facebook: The Role of Social Logins in the Online Advertising Ecosystem," 2017.

[18] T. Geethamanasa and M. N. Rajeswari, "Involving Community Media To E-Business Wintry-Commence Invention Proposal Using Microblogging Information," International Journal Of Innovative Technology And Research, vol. 5, pp. 6367-6369, 2017.

[19] S. Egelman, "My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, pp. 2369-2378.

[20] A. Hussain, N. L. Hashim, N. Nordin, and H. M. Tahir, "A metric-based evaluation model for applications on mobile phones," Journal of ICT, vol. 12, pp. 55-71, 2013.

[21] A. M. Lund, "Measuring usability with the USE questionnaire," Usability interface, vol. 8, pp. 3-6, 2001.

[22] H. A. Mahmoud and S. Hassan, "Using Microsoft Multipoint Technology and Interaction Design to Leverage Collaboration among Primary School Students," in The proceedings of 5th International Conference on Knowledge Management 2010, 2010, pp. 174-179.

[23] M. I. Sabri and A. Hussain, "Mobile recommender application for promoting electricity saving among Iraqis," in AIP Conference Proceedings, 2017, p. 020124.

[24] A. Hussain, M. Isam, and E. O. Mkpojiogu, "A UX Assessment of Mobile Recommender App for Household Electrical Energy Savings," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 9, pp. 23-27, 2017.

[25] M. N. F. A. Razak, A. Hussain, and M. M. F. Hamdi, "Usability study of youtube websites for Malaysian teenagers," in AIP Conference Proceedings, 2017, p. 020121.