Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015
11-13 August, 2015, Istanbul, Turkey. Universiti Utara Malaysia (http://www.uum.edu.my)

Paper No. 198

MOBILE QURAN APP SECURITY VULNERABILITIES

Shuhaili Talib, Murni Mahmud, Emilia Sarah Abd Rahman, Anis Suraya Songib, and Adamu Abubakar

Department Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia
{adamu, shuhaili, murni}@iium.edu.my, suraya.arrayyan@gmail.com, emiliasarahman@gmail.com

ABSTRACT. The security threats and vulnerabilities of mobile Quran applications can be viewed from both developers' and a service perspective. Similar to other apps categories like entertainment apps, games apps, banking apps and many others, understanding the threats and vulnerabilities of mobile Quran apps and the ways to manage them is crucial. With regard to the rapid transformation of many services and transactions onto mobile platforms, the security awareness of these becomes very important. Developers are responsible for ensuring that they have the necessary tools they need to build secure mobile apps which will secure and protect end user privacy and ensure reliable service delivery. Mobile Quran apps that provide features for enabling reading the Quran and interacting with other add-ons prolific events, like an easy and fast surah index list, efficient search features and many more need to be protected. Any attempt that could compromise the originality of the content of the Quran which is built for mobile apps needs to be identified. Unfortunately the security vulnerabilities within these features that convey the contents of the Quran are not clear, and there is a lack of noticeable security threats and vulnerabilities from previous studies. This paper examine the category of mobile Quran app and investigates its security threats and vulnerabilities. The outcome indicates measures to ensure that end users get the mobile Quran apps they need without compromising their privacy.

Keywords: mobile Quran apps, threat, security vulnerabilities

INTRODUCTION

The Quran is a revealed authentic sacred book from God, usually made available to readers in printed text format called Mushaf (Khan and Alginahi, 2013). Mobile Quran apps in the context of this study are an application that runs on smart phone platforms. The application either explores the Quran text or the Quran text is rendered in a video animation or recitation of the verses of Quran (in sound), as well as any other extra demonstrations that aim to teach users. This category of application that we are talking about here could also belong to digital Islamic products. They could be perceived as a Digital Quran Series. In this case, they are within the class of digital complete Holy Quran on a special device(s) or a special mobile device other than mobile phone. Some of these products come with a small screen, where they can explore the Quran text with a text Translation in Multi-Languages, as well as other Islamic Book Collections, and even Prayers Timings and Qibla direction. Such devices also contain a Tasbeeh counter. The combination of all these features is very exciting to users and serves to disseminate the teaching of Quran and Islam. Now with the proliferation of a mobile platform utilized for running many different applications, Quran and Islamic resources in digital form which were seen on dedicated devices are also developed and run on smart phones. These applications can be produce by anyone capable of writing programs. Currently, there are a number of Mobile Quran apps online for different mobile platforms, amongst which are those from iOS platforms as follows; Quran Explorer, Quran Touch HD with Tafseer and Audio (Al-Quran Al-Karim), alQuran 3, Al Quran Al Kareem with Tafseer (Tahfeem), Translation and Audio, Quran Majeed Free Edition, Quran Audio FREE for Muslim with Tafsir – Ramadan and many more. Some others are for the Android platform, which involves: Quran Android, Al-Quran al-Hadi, Al Quran Al Karim, MP3 Quran, Al Quran, Complete Quran (Indonesia), Mushaf - Quran Kareem, Quran off line, Al-Quran 30 Juz free copies, Holy Quran, Quran Android, Quran Bahasa Melayu, Al-Quran(free), MP3 Quran, Iqra' Al-Quran, Al Quran, Holy Quran, Al-Qur'an Bahasa Indonesia, Al-Quran Dan Terjemahan, iQuran Lite and many more.

Mobile apps are evaluated through different approaches based on set-up objectives. Given that they are produced for use in various fields, their functions rely on internal or external services and the implementation could be either for instant messaging, commonly available mobile instant messaging or it could be as an email client. Nowadays, there are many mobile payment applications that are used for transactions in business. Most of them take advantage of features like mobile browsing, near field communication, and mobile device networking resources capability. In the area of navigation aided systems, previous in-car navigation systems like Tom-Tom and Garmin are now deployed on mobile platforms serving similar purposes as earlier ones. Location based services are now commonly available for mobile devices. Day by day, we are witnessing a rapid increase in mobile applications for human endeavor that are providing various ranges of services. On-going research into these applications uses numerous ways to assess their efficiencies and weaknesses in questions. Some studies consider the evaluation of mobile apps on the System Usability Scale (SUS) (Donald, 2015) and the usability of applications (Fatih et al., 2013), while others focus on mobile users experience of design (Mendoza, 2014), and some on language learning and spelling ability enhancements (Ru-Chu et al., 2015), whereas in some cases, the performance of the application was emphasized when evaluating. This is seen in the evaluations of efficient reminder services (Chia-Yung, et al. (2014) and also in testing the response time under mobile platforms and network conditions (Rajan et al., 2014). Mobile apps have even been utilized even in biochemistry to separate protein molecule in polyacrylamide gel (Jakkrit et al., 2014) and also as a spectral Analyser (Evans et al., 2014).

For the purposes of this research, we seek to address the category of mobile Quran apps, in which whether as a special category (mobile religious apps), which is yet to be recognized, or as non-transactional, but providing services to the user. This proposition leads us to study the different classes of mobile apps. Furthermore, we investigate the security threat and vulnerabilities involves in mobile applications for the Quran in order to gather any form of suspicious act or irregularities that might be exploited. More emphasis is given to mobile Quran on client/server based

MOBILE APPS AND THEIR CLASSIFICATIONS

There are a large number of mobile Apps developed for various mobile platforms. A survey study indicated that as of the end of July 2013, there were over 1.9 million mobile Apps, and more than 100 billion cumulative downloads at Apple’s App store and Google Play (Zhu et al., 2014). To the best of our knowledge, there is no research output on the general consensus of the classification of mobile apps, although building mobile apps from whatever situation falls within the generic software development life cycle (SDLC), despite already existing conventions in terms of development or programming procedure for software by SDLC. Doolittle et al. (2012) proposed that a mobile application development framework include a decision matrix capable of exploring mobile development business value. Similarly, Maycock (2013) proposed an Enterprise Mobile Application Lifecycle process to include end-to-end lifecycle perspective in order to enhance the capabilities of subsequent productions. There could be more approaches to mobile application development than expected. Nevertheless, these evidences have indicated the importance of a generic process required in the development of mobile apps, as well as the impact of the developed product. In this sense, mobile applications can be produced under a specific development category for a certain set of services. As a result, a mobile application could serve many categories under "Mobile Games Apps, Mobile Entertainment Apps, Mobile Government Apps, Utility Apps" and many more. This has already gained a huge popularity on the part of users, and considers the services that mobile apps provided. However, when it comes to services that it provides, many issues could be raised. Heinonen and Pura (2006) consider the classification of mobiles apps to rely on the services that it will offer, viewing it from a customer-centric perspective. Herbjørn and Thorbjørnsen (2015) suggest a two-dimensional classification scheme for mobile application to be based the services interactivity and process characteristics which are associated with goal-directed vs. experiential services. Nickerson et al. (2007) consider the classification of mobile application to be based on real-time/non-real-time scale, aimed at retrieving informational and transactional processes. Kemper and Wolf (2002) classified mobile application systems under degree of innovation, speed of development, and risk. This classification is based on the analysis of prior categorization that grouped mobile applications into five classes as follows: mobile information, mobile transaction, mobile communication, mobile entertainment, and mobile services for special purposes like health, environment, and security services. On the other hand, mobile application can also be classify based on developers perspective. In this case, the development features and resources required are the major subjects. Therefore, mobile apps for this classification could be based on platforms, for examples iOS or Android platforms. The major resources that will be required for this kind of group of mobile apps is the Internet. They could either be accessed through a browser as a client side, as in google.com, or the application had to be installed on a mobile device before and then connected to the Internet before it runs, for example instant messenger. Other mobile applications do not need the Internet, like games. In general when considering mobile applications from developers' perspectives, they could either be in the client/server or client side application. Phuc (2012) suggests five developer's perspectives for a mobile app as follows: native apps, platform-based apps, mobile widgets, Web apps and HTML mobile apps.

The common link between developer's perspective and services perspective in terms of classification of mobile apps is the Internet. Smart phones are well-equipped with Internet-access-devices. This is why nowadays, the terminology "mobile Internet" is common in the mainstream. This gives a new way of engaging in online interaction transactions and has gradually changed Internet usage from the web context to the mobile context (Aiguo, 2013). Smartphone apps which utilized the Internet have been seen in many areas, and there is quite a lot of research on mobile Internet usage by Zhou, (2011) and Wang and Wang (2010).

MOBILE APP SECURITY AS APPLIED TO MOBILE QURAN

Security is everything. Users of mobile devices need to understand mobile App Securities and how to manage them. Due to the increase in demand for many transactions and services on mobile devices, security awareness of these mobile apps has become very important. Developers are responsible for ensuring the necessary tools to build secure mobile apps. This will allow them to procure or develop secure and manage applications while protecting end user privacy. The outcome will ensure that the end users gets the mobile apps they need without compromising on privacy. Some voluntary research committees like Open Web Application Security Project (OWASP) which are dedicated to improving the security of software has listed the top ten core mobile application security issues. Almost all of the types of mobile application security issues in OWASP are concerned with client server mobile applications. The most crucial mobile app security issues in their report of 2014 is weak server side control. This was number two in the 2013 report, and now it becomes the first. This particular type of security threat is related to mobile enterprise applications. The fact remains that the client side must rely on some sort of back-end services. It is crucial to take similar steps used on traditional server-side security on web application for mobile application. Based on the top 10 of OWASP, the remaining security issues are also crucial, and could be devastating when they strike. In addition, while the threats remain fairly similar, the abilities of attackers who manage to get control of a mobile device are much different, and may be much worse. The fact that the Quran is a sacred book, and it is required to be read by all Muslims, and is the backbone of Islamic belief, ethics and values, and that any mobile developer can develop it, makes it vulnerable to tampering and alteration. This is a serious problem for mobile Quran apps. Instead of doing good, they might now cause harm of someone alters or modifies them. The content at this point is compromised and readers are unaware that this result is the major problem. The consequence of mobile Quran app security threats and vulnerabilities is not like that of the other categories of mobile app. In some mobile apps like banking, there could be a loss of money and property, whereas in mobile Quran apps, the main threat is modifications and deceptions. We need to detect all possible angles where such modification can happen. We also need to be very cautious in cases of deceptions. As a result, the possible threats and vulnerabilities involved in building mobile applications for the Quran using existing components that contain some form of any suspicious act of irregularity might be exploited.

METHODOLOGY

In order to further examine the security threats and vulnerabilities, this evaluation focused on mobile Quran apps available in the public domain, that is, those that are found online. The key evaluation parameter was the features found on those apps that are prone to security jacking. This was a qualitative exploratory approach, where subjective assessment of features were captured as indicators of complex security issues and we attempted to understand these security complexes from the viewpoint of both developers and users. In the domain of security, a qualitative approach helps to use inductive methods to gather information that represent what might be realistic attributes of the vulnerabilities phenomenon. Most often, the ultimate goal of the qualitative approach is that of theory building, which leads to the formulation of a theoretical explanation that specifies a poorly understood phenomenon (Strauss & Corbin, 1990). Yet qualitative methods can also be used to test a theory (Ketchen & Berg, 2006).

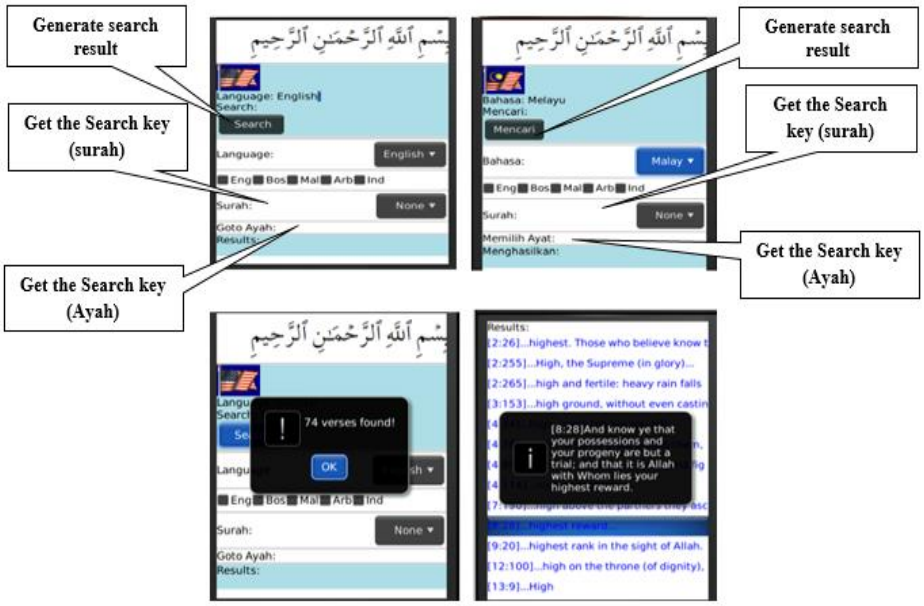
Evaluation Procedure

The evaluation procedure is presented in Figure 3. Mobile apps were downloaded from the Internet and installed on a smartphone and a tablet. Some of the apps were on an Android platform (Redmi Note 4G), whereas others are on iOS platform (iPad). The evaluation involved an examination for extracting features that would be vulnerable to the security loopholes of the mobile Quran app. These features were deemed to represent areas of consideration. The conceptual approach to evaluation strategies of mobile Quran apps security was then formulated, followed by a process of browsing and exploring every mobile Quran apps found. The steps for the evaluations mainly followed the guide from the conceptual strategies designed.

Conceptual Strategy for Evaluation of mobile Quran apps security

We conceptualized an evaluation approach for the mobile Quran apps available online. We first studied the available mobile apps online. Thereafter, we came up with the idea of going bit-by-bit and exploring all the aspects which made the mobile Quran apps looks vulnerable.

For example in Figure 1 and Figure 2, the point where there could be problems within those mobile Quran apps was "*Generate search result for surah, ayah and reciter"* and (here), we explored some of the selected evaluated parts where mobile Quran apps might be attacked. Our argument was based on the fact that the mobile Quran apps seen in Figure 1 and Figure 2 were on client server platform and they could also be on the client side alone. This fact is based on exploring all vulnerability angles. Meanwhile, the developer's side was also considered in terms of the "requests", where for each generation of surah, ayah or reciter, something else could be the output, which might be altered. There was a strong possibility of Client Side Injection and Data modification as a result of Weak Server Side Control. These were also serious securities issues which were part of the OWAPS top 10. The Quran contents might thus be compromised and it would be difficult for this to be detected by the end user. As a result, many alteration or modified version of Quran contents for mobile device might be delivered to the public.



74 verses found!

[2:26]...highest. Those who believe know t
[2:255]...High, the Supreme (in glory)...
[2:265]...high and fertile: heavy rain falls
[3:153]...high ground, without even castin
[9:20]...highest rank in the sight of Allah.
[12:100]...high on the throne (of dignity).
[13:9]...High

[8:28]And know ye that your possessions and your progeny are but a trial; and that it is Allah with Whom lies your highest reward.

Figure 1. Mobile Quran apps Interacting Feature that might leads to security threats

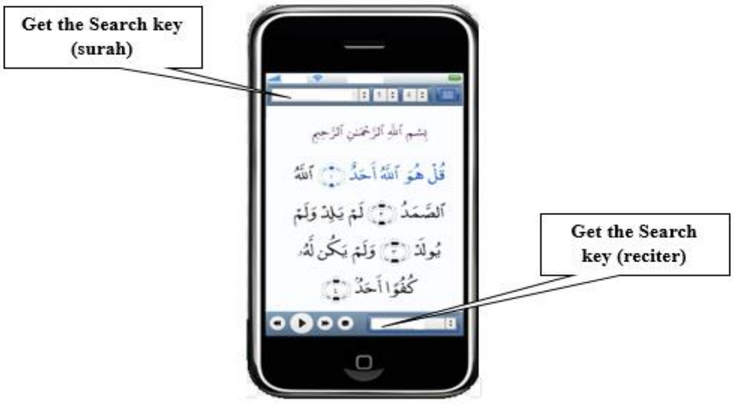

Get the Search key (surah)
Get the Search key (reciter)
بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ
قُلْ هُوَ ٱللَّهُ أَحَدٌ ٱللَّهُ ٱلصَّمَدُ لَمْ يَلِدْ وَلَمْ يُولَدْ وَلَمْ يَكُن لَّهُۥ كُفُوًا أَحَدٌ

Figure 2. Mobile Quran app: Exploiting security concerns

Evaluation of mobile Quran apps security

Mobile apps were subject to a rigorous focus on usage and usability. Although some research were able to come up with some evaluation strategies aimed at looking it from developer's point of view. For example, Phuc (2012) evaluated mobile apps from the developer viewpoint, based on a set of selected criteria. The study was able to produce a developed mobile app, to include the evaluation claim of producing a paradigm that fits better to a certain type of app. Furthermore, subjective analysis on user studies was also claimed to provide valuable results in terms of understanding the state of the issue at hand. Similar to this, is the work of Claudia and Harrison (2013), which was able to provide a Mobile App Review Analyser` that is capable of gathering feedbacks reported by users and further analyze them, in order to identify a common theme across the users' responses. For this research, possible vulnerabilities are the set-up objectives. They are explored from the general view point of the security threat and vulnerabilities of software. Hence, some sample of mobile Quran apps available in public domain, are evaluated for security threat and vulnerabilities using the steps shown in Figure 3.

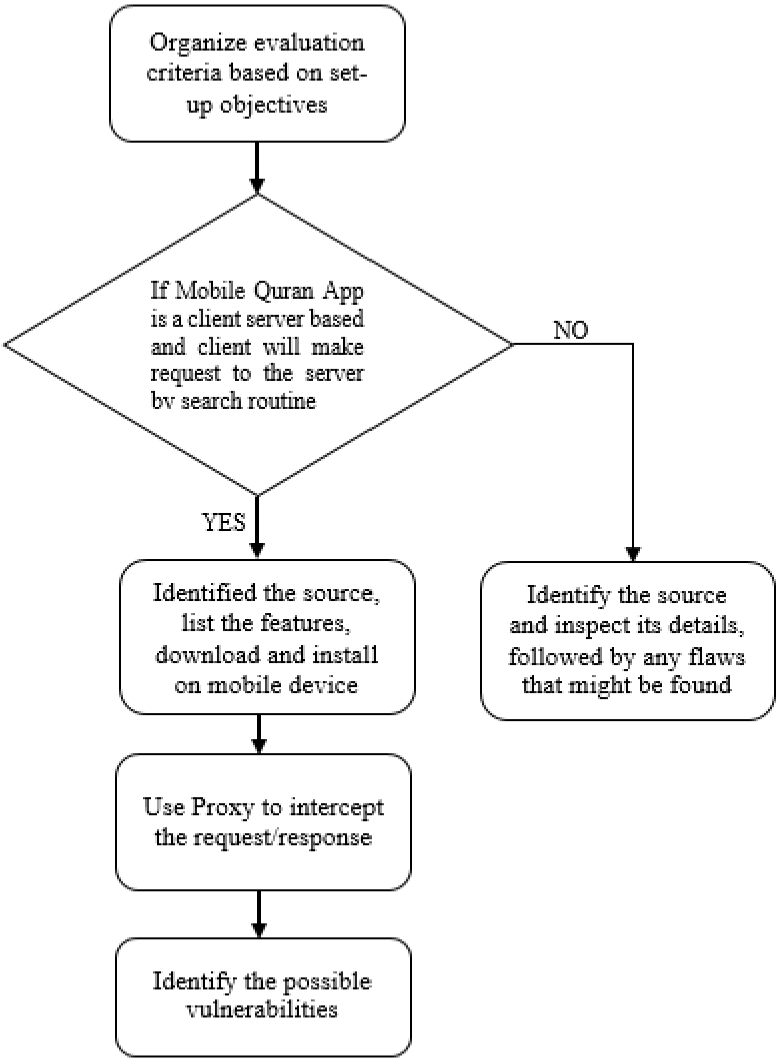

Organize evaluation criteria based on set-up objectives
If Mobile Quran App is a client server based and client will make request to the server by search routine
NO
YES
Identified the source, list the features, download and install on mobile device
Identify the source and inspect its details, followed by any flaws that might be found
Use Proxy to intercept the request/response
Identify the possible vulnerabilities

Figure 3. Flowchart of the evaluation approach

With focus to request/response from client mobile Quran application to Server and vice versa. This study outline the evaluation of security to beings by organizing evaluation criteria based on set-up objectives. The objective for this study is to evaluate the likelihood with which Quran content might be alter/modify while on transit from client to server. For this reason, a proxy server was used. First we begin by identifying the source of each mobile Quran apps and listing their features. If Mobile Quran App is found to be on a client server based, it was then downloaded and installed on mobile device. Otherwise, we identify the source and inspect its details, followed by any flaws that might be found. In both cases, it will lead to the identification of any flaws that might occur.

RESULTS

The results of the evaluation analysis detected that some mobile Quran apps followed the conceptual strategies we designed. We were able to find mobile apps that provided a search properties criterion and are on client server based. These were thus treated as "extreme" security loopholes that could lead to the extraction of modified or altered Quran app contents. Consequently, this could cause problems to users. The first mobile Quran app to be evaluated was "**Quran Android".** This is a mobile Quran app produced by the **"Language Research Group, University of Leeds".** We observed a search text box is provided for any keywords. Related results/verse of Quran will then displayed, and users could choose only to download the selected data (reciter, tafsir, translation). There is great support and also a forum community alongside the apps. Crucial to security concern is that the apps was pre-process for Arabic grammar, syntax and morphology for each word in the Holy Quran. This is exactly where we might point out a loophole, however, because users who can search to explore a keyword might be affected by client side injection and data manipulation. The claim here is that users might not be sure that the return value is a true or altered value, hence security features becomes very important. The second mobile Quran evaluated was "**Al-Quran al-Hadi",** developed by **"Pusat Kajian Hadis, Jakarta".** Rather like the previous one, this also contains a Search result for a keyword, and is categorized into several topics. Users can choose to only download selected data (reciter, tafsir, translation). The third one is "**Al Quran Al Karim"** developed by "**Mohamed Dahrough".** It is a simple app, suitable for people who only want to read the Quran using a smartphone. The size of the apps is also small. The Quran's appearance looks like a real hardcopy of the Quran. The major security concern here is the content validity state, in the sense of whether it is modified or not. The fourth mobile Quran app to be evaluated was the "**MP3 Quran"** developed by the **"Ultimate Vision, SP-Apps.com"** There are options to users in terms of which reciter and which verse to be explored. This is similar to the first two evaluated apps, and the same security situations also applied here. The fifth mobile Quran evaluated is "**Al Quran"** it is developed by **"Islamic Apps"** this is also possess similar security loopholes from the first two evaluated. However, all its features are on one page. Users can download audio for selected surah of selected reciter only, and there is no need to download all. The sixth mobile Quran evaluated was called "**Complete Quran (Indonesia)"** developed by **"Badr Interactive". T**he security situation here is similar to the first two evaluated apps. The app comes with guidelines for usage. The seventh mobile Quran Evaluated was called "**Mushaf - Quran Kareem"** Developed by **"Wail Busaied",** this is very similar to the third evaluated, and the security situation of the third also applied here. The eighth mobile Quran evaluated is called "**Quran Explorer"** developed by **"Noble Education Foundation, Inc".** The security situation here is similar to the first two evaluated. Finally "**alQuran 3" developed by "Sayed Samed"** was evaluated, and found out to have similar security loophole as the first two.

This results suggest that users should be aware of the security vulnerabilities within these features. The developers need to convey an assurance that the contents of their Quran apps are pure, and upon searching and interacting, will yield a reliable result. This study identified these issues as security threats and vulnerabilities that could lead to modifications and alterations of mobile Quran apps. This paper examines the category of mobile Quran app and investigates its security threat and vulnerabilities. The outcome indicates measures to ensure that the end users gets the mobile Quran apps they need without compromising their privacy.

CONCLUSION

This study creates an awareness of the possible loopholes that mobile Quran apps could be vulnerable to in regards to alteration and modification of the contents of the Quran. The study started by categorizing mobile Quran apps and investigating the state of its design and content. Mobile Quran apps that are widely available for most smartphone platforms in public domain were collected. Security threats and vulnerability issues were then conceptualized. Based on this conceptualization, an evaluation was performed to investigate the security vulnerabilities within these features' conceptualized framework. The results indicate that developers need to convey an assurance that the contents of their mobile Quran app were credible, and even upon interaction with add-on features, would not jeopardize content validity. This study makes it clear that identifying issues related to security threats and vulnerabilities could alleviate modifications and alterations that might occur on mobile Quran apps. Finally, the outcome of the study indicates measures to ensure that the end users get the mobile Quran apps they need, without compromising their privacy.

ACKNOWLEDGMENTS

This research was supported by the International Islamic University Malaysia (IIUM) Research Acculturation Grant Scheme (RAGS) 14-051-0114.

REFERENCES

Aiguo, L. (2013). Mobile library service in key Chinese academic libraries. *The Journal of Academic Librarianship* 39(3), 223-226.

Chia-Yung, L., et al. (2014). Improvements in dental care using a new mobile app with cloud services. *Journal of the Formosan Medical Association* 113(10), 742-749.

Claudia, I. & Harrison, R. (2013). Retrieving and analyzing mobile apps feature requests from online reviews. *10th IEEE Working Conference on Mining Software Repositories (MSR)*,IEEE.

Donald, C. M. (2015). Usability assessment of a mobile app for art therapy. *The Arts in Psychotherapy*, 43(1), 1-6.

Doolittle, J., Moohan, I. A., Simpson, J., & Soanes, I. I. (2012). Building a mobile application development framework, *Intel Whitepaper. Available online: http://communities. intel. com/docs/DOC-19555 (Retrieved February 20th, 2015).*

Evans, M. J., Clemens, G., Casey, C., & Baker. M. J. (2014). Developing a mobile app for remote access to and data analysis of spectra. *Vibrational Spectroscopy* 72, 37-43.

Fatih, N., Desharnais, J-M., & Abran, A. (2013). An Expert-based Framework for Evaluating iOS Application Usability. *Proceedings of International Workshop on Software Measurement and the 2013 Eighth International Conference on Software Process and Product Measurement (IWSM-MENSURA), 2013 Joint Conference of the 23rd.*

Heinonen, K., & Pura, M. (2006). Developing a Conceptual Framework for Mobile Services. *Proceedings of the Helsinki Mobility Roundtable*, Helsinki, Finland.

Herbjørn, N., Pedersen, P. E. & Thorbjørnsen, H. (2015). Intentions to use mobile services: Antecedents and cross-service comparisons. *Journal of the academy of marketing science,* 33(3), 330-346.

Jakkrit, J., et al. (2014). Implementation and evaluation of SDS-PAGE image analysis on a mobile app. *International Conference on Computer Science and Engineering Conference (ICSEC).*

Kemper, H. & Wolf, E. (2002). Iterative Process Models for Mobile Application Systems: A Framework, *Proceedings of the 23rd International Conference on Information Systems*, Barcelona, Spain, 401-413.

Ketchen, D. J., & Bergh, D. D. (2006). *Research methodology in strategy and management*. Amsterdam: Elsevier JAI.

Khan M. K., & Alginahi, Y. M. (2013). The Holy Quran Digitization: Challenges and Concerns. *Life Science Journal*, 10(2).

Mavcock, D. (2013). Enterprise Mobile Application Lifecycle Developing a Process for End to End Mobile Application Development, Slalom Consulting. *Available online: http://www. enterprisemanagement360.com/wp-content/files_mf/1341922927entlifecycle.pdf(Retrieved February 20th, 2015)* (2013)

Mendoza, A. (2014). Mobile App or Mobile Web: The Big Debate, *Mobile User Experience*, 161-173

Nickerson, R., Varshney, U., Muntermann, J., & Isaac, H. (2007). Towards a taxonomy of mobile applications. *Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado*, USA, August 9-12.

Phuc H. U. (2012). Developing apps for mobile phones. *7th International Conference on Computing and Convergence Technology (ICCCT),* IEEE.

Rajan, V. S., Malini, A., & Sundarakantham., K. (2014). Performance evaluation of online mobile application using Test My App. In *International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 1148-1152.

Ru-Chu, S., Lee, C., & Cheng, T. (2015) Effects of English Spelling Learning Experience through a Mobile LINE APP for College Students. *Procedia-Social and Behavioral Sciences* 174, 2634-2638.

Strauss, A. L., & Corbin, J. M. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Newbury Park, Calif.: Sage Publications

Wang, H. Y., & Wang, S. H. (2010). User acceptance of mobile internet based on the unified theory of acceptance and use of technology: Investigating the determinants and gender differences. *Social Behavior and Personality: an international journal*, 38(3), 415-426.

Xu, J., et al. (2013). MobSafe: cloud computing based forensic analysis for massive mobile applications using data mining. *Tsinghua Science and Technology*, 18(4).

Zhou, T. (2011). Understanding mobile Internet continuance usage from the perspectives of UTAUT and flow. *Information Development* 27(3), 207-218.

Zhu, H., Chen, E., Xiong, H., Cao, H., & Tian, J. (2014). Mobile app classification with enriched contextual information. *Mobile Computing, IEEE Transactions on* 13(7), 1550-1563.