Security Issues in the Use of Mobile Educational Apps: A Review

https://doi.org/10.3991/ijim.v15i06.20631

Emmanuel O.C. Mkpojiogu (✉)
Universiti Utara Malaysia UUM, Sintok, Malaysia
Veritas University, Abuja, Nigeria
emmanuel10178@yandex.com

Azham Hussain
Universiti Utara Malaysia UUM, Sintok, Malaysia

Monday Onah Agbudu
Veritas University, Abuja, Nigeria

Abstract—Although, there are several literatures pertaining to the security issues in the use of mobile apps, these literatures do not sufficiently address issues about the security challenges in the use of mobile educational app. Hence, this work attempts to review the available literatures with the aim of capturing the security issues in the use of mobile educational apps. To achieve the stated research goal, the study applied systematic literature review methodology. Sixty-four (64) papers in the area of security issues in the use of mobile educational apps were downloaded. Out of these papers, twenty-one (21) most relevant studies were selected for review in order to extract the appropriate information needed for the analysis. The results from the review reveals the scarcity of appropriate literatures on security issues in the use of mobile educational apps and that these issues are a thing of concern, and needed to be looked into in this ever-growing world of technologies. However, most of the studies, taken single handedly reviewed lack of comprehensive framework to demonstrate the security challenges in the use of mobile educational apps. Thus, the results from this paper provide additional knowledge to the users of mobile apps as a whole; students in their usage of mobile educational apps and the research community on the current security challenges in the use of mobile educational apps.

Keywords—Mobile apps, mobile devices, educational apps, security issues

1 Introduction

The Increase and rapid growth of portable computers and mobile devices that can be connected to wireless networks have facilitated mobility and mobile learning [27], and have heralded both opportunities and challenges for educational institutions and their teachers and learners [3]. Mobility in this sense, gives the corollary an extension

beyond the traditional way of learning, which gives a huge range of diverse opportunities, and is well positioned for the delivery of student support interventions [5]. Hence, due to the fall in prices of these technologies, mobile phones in particular, many people, even in impoverished areas, can now afford and know how to use mobile devices to aid learning [26]. According to the 2013 UNESCO Report, mobile technologies are commonly found nowadays even in areas where schools, books, and computers are scarce. This increasing availability of low-cost mobile and wireless devices, with more educational apps being developed, are arguably well positioned to play a more central and effective role in providing students with much needed information, and conversation theories that can be adapted for a mobile learning situation [17]. Mobile learning (m-learning) in this sense is a research domain that analyzes how mobile devices can contribute to learning [3][28]. Thus, m-learning involves the use of mobile technologies, either solely or combined with other communication and information technologies to allow learning anywhere, and at any time [26]. However, given the growth in mobile technologies, and educational apps, the formation of a usable and accessible mobile learning system has also posed security concern to all [5]. With this picture therefore, [17] argues that it is necessary to establish restrictions to the use of mobile devices in schools in order to have a better development of the pedagogical actions, and also to "slow down" students from the hectic pace of contemporary life. However, he also considers it realistic to incorporate this equipment into the various educational projects. Consequently, even though some works have been done in the use of mobile educational apps, and security issues in the use of mobile applications, little have been done in the security issues affecting the use of mobile educational apps. Thus, this paper brings to consciousness the security issues arising from the use of mobile educational applications like protection of confidentiality, integrity, reliability, trust, privacy and availability of information; and at the same time proffering ways of combating with these challenges.

Information security is often viewed as the protection of confidentiality, integrity and availability of information [3], but without adequate knowledge of this, vulnerabilities becomes the order of the day. Therefore, this study intends to elucidate the security challenges in the use of mobile educational apps. That is, to create a security concern and awareness in the minds the users of mobile educational apps and at the same time proffering ways of tackling these security issues. We live in a world where there is constant growth in the use of mobile devices for variety of applications, ranging from education, finance, healthcare and the likes. It becomes necessary therefore, to create security awareness in the mind of the users of these apps. The objectives of the work therefore are: i) To elicit the security issues in the use of mobile educational apps; ii) To find out ways of handling the security issues in the use of mobile educational apps. The following research questions will guide this study; i) What are the security challenges in the use of mobile educational apps? ii) Are the users of mobile educational apps aware of these security issues? and iii) What are the possible ways of handling these security challenges? Often, the users of mobile devices are not aware of the probable security threats they are expose to, or they are ignorant of their own shortcomings or their potentially unsafe behavior. If not, they

would have behaved more securely when their security awareness is raised. Thus, the purpose of this study is to promote secure behavior and enhance security awareness among the users of mobile educational apps. This study is significant as it will help in the design and evaluation of mobile educational apps, thus, improving the reliability, and usability of mobile educational apps [7-11]. More so, this study can be extended to explore other aspects of instruction such as distance learning and advanced online learning. The growth of modern mobile educational apps is of no small measure a great help to the student community, to keep the availability of needed resource on their hand. No wonder then [13] posit that using mobile apps in education seems to be inevitable in today's classroom. Consequently, the scope of this work is centered on how secure the users of these mobile educational apps are against the third party. That is, what challenges do the security issues of using mobile educational apps pose, and what are the possible remedies. The remaining content of this work is organized thus, section 2, is the literature review, section 3, deals with the methodology, while section 4, deals with the result, section 5, discusses the findings, and section 6, the general conclusion which includes the recommendation and future work.

2 Literature Review

2.1 The use of mobile educational apps

Learning in its wider perspective could be seen as a continuous process of enriching the human knowledge, of which focus has now completely shifted to eLearning. Due to the mobile phones and the various feature-oriented applications, students can learn at their pace and take their time at understanding things, as everything is just a click away [29][21]. In these changing times thus, students are more driven towards using a mobile phone for every purpose, or a smartphone as commonly called [23]. More so, the world is at the fingertips and a student can get access to any information from anywhere. This reduces the chance of visiting a library and searching for the data, since a mobile phone can be used for a number of such purposes. However, what makes the information easily available is "mobile applications" [3]. Hence, every mobile app has a unique feature which offers its own set of services.

2.2 The important role of using mobile apps in education

Mobile applications (apps) have gradually brought about some crucial changes in the education industry, as most of the institutions, tutorial centers, and individual educators are getting in touch with the apps stores, to get the mobile apps for imparting knowledge, and this is because the educational apps offer a lot of benefits [12]. Thus, mobile apps have progressively become the most interactive and constructive way to attract students towards studies and enhancing their productivity. The following therefore could be seen as some of the important role of using mobile educational apps:

Interactive learning: Gone are the days, when the only option for the students to read books, was by visiting the library (the traditional settings). On the other hand, the innovative gadgets of today make it easy for students to practice their lessons in an effective and interactive way [24]. These become readily possible through the use of apps in mobile gadgets, and are available for all types of skill levels and aid learning using a variety of teaching methods, such as video tutorials, and even the educational games [6]. These apps ensure interactive and effective learning, by transforming the boring lessons and helping the students to visualize each and everything.

Availability: Unlike schools, the mobile apps are available round the clock. Therefore, learning via apps is not a time-bound learning; rather it is a relaxed learning [12]. Consequently, time-bound learning is not much effective, as children get distracted very easily and are not able to concentrate continuously for a long time. Thus, educational apps work the best regarding this issue, as they are always available, and the students can study as per their convenience [24].

Ebooks and online study material: With the advancement of technology and introduction of educational apps, students are not required to invest their time and money to buy the required study material from bookshops and libraries. These educational apps help the students who are unable to visit the library on a regular basis, by providing required study material in just a few clicks [1]. Educational apps also help the readers to discover a variety of eBooks with a mere click.

Portability: Mobile devices could be said to be an important part of our everyday lives since they enable us to access a large variety of ubiquitous services, a reason why most persons will not leave their mobile phones at home while going somewhere [1]. Thus, using apps have become a part of the daily routine, whether one is watching a video on the way to work or playing games at lunch, one's phone is always with him/her. Therefore, the apps can be the constant companions for the students, that is, with the help of educational apps, learning will not be confined to the classroom alone, as the apps allow pupils to take their learning into their own hands and they can study and test themselves at any point in the day [24].

Individually-focused learning: A teacher's role in the student's life is not at all questionable, but a teacher cannot focus towards one student only. He/she typically has to engage with 20-30 pupils during each session, and it is difficult to ensure each one is engaged and following what is being taught. However, when a student utilizes an app, the time they interact with the app is all their own [2].

Instant updates: There are apps, which are not only meant for learning but also to stay updated about the campus events, timetables, alerts and other important information. These apps help the children as well as their parents to get instant updates regarding the important things, which they may miss otherwise [5].

The above-mentioned benefits or importance are enough to prove the worth of the educational apps, but the apps have a lot more to offer. Hence, without any doubt, technology has helped a lot to create a global platform for education as well as helped to identify the hidden skills and talents of the students.

2.3 Security issues in the use of mobile educational apps

With the increasing use of mobile devices and applications for storing or accessing personal and sensitive information, many users are not aware of the growing security threats in using these devices and many users are also not aware that some mobile apps are not so secure [22]. As such, as more people use smartphones and tablets for their educational and financial activities, the more attractive these devices and their applications become targets to attackers with mischievous intents. Hence, recent security surveys have reported a rapid increase in the number of mobile threats and the growing sophistication of the attacks [4]. Consequently, this section discusses the security concerns associated with mobile learning:

Reliability: Though educational technology advances at a rapid pace, but the internet infrastructure in many educational institutions often gets overwhelmed when accessed by so many devices at the same time [16]. This is why school management need to ensure its capacity is updated. What is more, they have to develop a plan B for any user that might encounter some trouble with chargers and shared power outlets. Needful to know is that rapid pace of change in terms of mobile devices adoption in the classroom has sometimes obscured thoughtful evaluation of the efficacy of current mobile learning strategies or the examination of how and why certain types of implementations affected student achievement more than others [4]. Thus, mobile learning is never a stand-alone activity, and so can be really challenging for teachers to pinpoint exactly how the use of mobile devices in the classroom has improved the students' academic performance or not.

Integrity: Most notably, school and district administrators are struggling with how to elevate the use of the devices from sporadic, engagement activities, to instructionally rich learning experiences. It is one thing to put mobile devices into students' hands and a totally different one to use the said technology in the most effective way possible [4]. The journey of mobile learning in the classroom has only begun and it is up to every educator to find the value of it [16]. Hence, the integrity of the mobile educational apps is called to question as educators need to make sure the mobile devices in the classroom are not used for other purposes than learning. Though however, smartphones and tablets remain communication devices after all, this does not mean students will always get distracted, as an interesting learning activity will keep them engaged and using their mobile devices to enhance their learning [22].

Some mobile operating system does not fit with the security software (trust): A mismatch between mobile devices' new operating systems and security software offerings can also cause a potential security risk. Sometimes, security software for mobile devices may not work with the integrated IT security systems already in place [19]. This can allow unsecure files to infiltrate the organization's network, thereby, killing the trust of its users.

Users' privacy/confidentiality: The recent technological advancements and unprecedented spread of mobile educational apps have created a lot of confident in its users; little do they know that mobile device can be hacked into, be misplaced or stolen. And as such cases, one's personal information and work data may fall into the wrong hands or a third party.

Availability: Although, mobile educational apps through mobile devices have achieved a high penetration rate in the world of today, the question still remain: "are they always available to its users"? That is, is the cost implication a hindrance to its users? Is installing it a difficult process? Does it take note of humanity as a whole, putting the less privilege ones into consideration? (Stallings & Brown, 2012). This thus, calls for availability of the mobile educational app, making it a source of security issue.

2.4 Need for security or way forward to security issues / threats

In the wake of the explosion of mobile devices, there is one critical question that many users continue to overlook: "are mobile apps secure and protected from malicious hackers?" This is because information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Maintaining privacy in our personal communication is something everyone should desire. This section therefore highlight some of the basic way forward to address the security issues in the use of mobile educational apps:

Making devices risk aware: An app's security is deeply impacted by the underlying device's security. An unsecured device is one that has been modified by its owner or an unauthorized app to bypass operating system security, in turn allowing the installation of any app and from any source (Brinda, & Bala, 2017). Such devices, known as "jailbroken" or "rooted devices", are very susceptible to mobile malware (Gbenga, 2006). To address these issues therefore, it is incumbent on users to adopt technology that will allow device risk to be incorporated into mobile application structure and detect mobile malware. For example, if an app were to execute a sensitive transaction – and the device is rooted or jailbroken - the app may elect against executing the task [4]. Thus, by making apps "device risk-aware," users can restrict certain functionalities, remove sensitive data, and prevent access to enterprise resources.

Preventing data theft and leakage: When mobile apps access personal data, documents are often stored on the device itself. If the device is lost, or if data is shared with third-party, the potential for data loss is heightened. Hence, a "selective remote wipe" should be developed, which is capable to erase sensitive data from stolen, lost, or a third-party mobile device [17]. Also, restricting the sharing of personal data with third-party apps can help prevent data leakage. More so, installing security apps such as phone tracking apps can come to your aid in case of theft or the loss of mobile devices [17].

Do not fall for 'free' traps: Who does not love free Wi-Fi, but avoid accessing mobile learning modules with unsecure connections will save a great deal. Some unsecure, unverified wireless connections put your personal information at risk and prone to hackers' attacks [25]. Hence, security consciousness is making sure your Internet service connection is safe.

Protect mobile devices with passwords and biometrics: Giving authorized access through user ids and passwords can prevent unauthorized access to mobile

learning content. Providing biometric access is a much safer mechanism [19]. Users also need to follow the standard procedures while creating their passwords to access mobile learning materials. The principle of having one capital letter, at least one special character and a minimum of 8 letters should be adapted for passwords [16]. Also, automatic logout settings with a minimum time frame should be activated when mobile learning modules are kept open idly.

Install malware protection mechanisms: To avoid virus/malware attacks, mobile devices and servers should use stringent protection mechanisms. Installing genuine/authorized anti-virus software programs with frequent updates, firewalls activation can keep one's mobile learning systems safe from attacks [12]. More so, having regular data backups and maintenance activities for m-learning servers can also prevent security threats [25].

Encrypt data for safety: In case of misplace or theft, if personal details and m-learning training material is in an encrypted form, one will be safe. Even if it falls into the wrong hands, that wo not be a problem, as the data cannot be decoded instantaneously; meanwhile, the individual can block the mobile device with the help of the International Mobile Station Equipment Identity (IMEI) number [12].

Provide security awareness training: Training managers need to make users aware of possible security threats and how to avoid them. Prevention they say is better than cure, and this is applicable in this context. Hence, instead of insisting on more sophisticated software programs, little precautions can avoid big damages [25]. Precautions like, keeping strong passwords, patterns, not allowing others to access your phones, utilizing the inbuilt security options such as blocking phone access in case of theft, all these little deeds count when we talk about security and privacy [12].

3 Methodology

In an attempt to find the existing literature that deals with security issues in the use of mobile educational apps, this study employs a systematic literature review approach to search for the relevant journals and conference proceedings on mobile educational app. Therefore, the anticipated activities in the systematic review include: Planning the review as a first stage, conducting the review as a second stage and finally result presentation. However, once the three stages have been achieved, the results of the analysis will then be presented.

3.1 Planning the review

The aim is to collect important and appropriate information related to security issues in the use of mobile educational apps. In this regard the search and selection strategy is defined as primary and secondary search. The primary search was carried out using internet database for high-ranking journals and conference proceedings in the area of mobile educational apps and security issues in the use of mobile educational apps. In this review, the search terms were selected based on a scope focused mainly on security issues in the use of mobile educational apps. The search

was carried out employing the following search strings, inter alia: **S1** ("security issues in the use of mobile educational apps"), and **S2** ("Mobile educational apps"). Therefore, the full string utilized in the review was: **S1** and **S2.** The secondary search was carried out through the citation and references obtained in the course of primary searching. However, emphasis was given to recent studies ranging from the year 2006 to 2019. This will provide current issues on security issues in the use of mobile educational apps. Literature on the security issues in the use of mobile educational apps are however, very limited. Table 1 below describes the selected journals and conference proceedings. The papers selected for the review were gotten from the following journals and conference proceedings recorded in table 1 respectively:

Table 1. Selected journals and conference proceedings

Journals	Conference proceedings
International Journal on New Trends in Education and their Implications	Conference for Educational Technology Research and Development.
Journal of International Technology and Information Management	Education Trust Fund Capacity Building for Knowledge-driven Growth for Nigerian Universities
International Journal on Integrating Technology in Education.	Issues in Informing Science and Information Technology
International Journal of Computer Applications,	Conference for Innovative Practice in Higher Education
Journal of Global Research in Computer Science	Conference Proceedings, Dar es Salaam, Tanzania
International Journal of Innovative Research in Information Security	International Conference on ICT for Africa
International Journal of Engineering Research and Application	The challenges for mobile learning in the classroom and how to overcome them.
International Journal of Social Media and Interactive Learning Environments	Use of mobile apps for teaching and research
	Use of educational apps in today's classroom.
	UNESCO Policy guidelines for mobile learning.

Table 2. Number of papers per journals and Conference proceedings

journals and conference proceedings	no. of paper
IJITE	1
IJIRIS	1
JGRCS	1
IJCA	1
IJNTEI	2
JITIM	1
CETRD	1
ETFCBKGNU	1
IISIT	1
CIPHE	1
CPDST	1
ICIA	2
CMLCO	1
UMATR	1
UEAT	1
UPGM	2
IJERA	1
IJSMILE	1
Total	21

The selection of appropriate papers for both journals and conference proceedings centered mostly on the research topic "security issues in the use of mobile educational apps". However, the review procedure was centered on the keywords: security issues, mobile educational apps and educational apps. Therefore, all the related and appropriate papers have been carefully selected for effective review and data extraction (see Table 2). Table 2 thus, displays the number of papers selected per journal or conference proceedings. The range of papers selected per journal or conference proceedings is from 1 to 2.

3.2 Conducting the review

In this phase, the papers selected were downloaded using the study's search string, and the abstract of each was carefully read in order to examine its relevance to this study. Sixty-four (64) works were downloaded from both journals and conference proceedings. However, only relevant papers with significant contributions were selected for further reading, as such only twenty-one (21) papers were considered. The 21 papers that were subsequently selected were then thoroughly read, searched, and studied for relevant detailed that pertain to subject matter of the review. Important and needful information (related to security issues in the use mobile educational apps) were extracted, collected and summarized. These formed the basis of the analysis presented in the results section. Thus, Table 3 shows the complete list of selected papers, these selected papers spanned from 2006 to 2019. These papers provided a good coverage of the literature collated after a keen selection from the 64 downloaded

papers on the reviews subject matter. The next section is the results and discussion section, where the results from the literature review were presented and discussed.

Table 3. List of selected papers

Paper ID	Authors	Year
Z1	Agbatogun, A. O.	2013
Z2	Gbenga, A.	2006.
Z3	Jegede, P. O.	2009
Z4	Stallings, W., & Brown, L.	2012
Z5	Kneil-Boxley, S.	2012
Z6	Adedoja, G., Botha, A., & Ogunleye, O. S.	2012
Z7	Osang,B.F., Ngole, J. & Tsuma, C .	2013
Z8	LIVA BRAN	(n.d.)
Z9	Batista, S. C. F., & Barcelos, G. T.	2014
Z10	Hinze, A., Vanderschantz, N., Timpany, C., Cunningham, S. J., Saravani, S., & Clive, W.	2017
Z11	Jayaprakash, S. & Chandar, V.	(n.d.)
Z12	Machado, J. L. A.	2012
Z13	UNESCO	2013
Z14	Barcelos, G. T.	2014
Z15	Shaibu, A. S. & Mike, J.	2016
Z16	Shabnam. K. K. & Mazleena, S.	2015
Z17	Prashant, K . J., Arnab, G. and Shashikant, R.	2013
Z18	Priyanka, G., Sahil, B., & Ajit, S.	2010
Z19	Indrajeet, M. K.	2016
Z20	Brinda, S. & Bala, P.	2017
Z21	Oyelere, S. S., Paliktzoglou, V., & Suhonen, J.	2016

In carrying out this research, different database were used such as Academia.edu, Google search and Google scholar. In the three-database used, the total number of 64 articles were found, and 21 articles were finally selected for the research work. Table 3 below shows the different database consulted and the total number of articles used.

Table 4. Database and selected articles

Database	Articles found	Articles selected
Google scholar	19	7
Academia.edu	34	11
Internet Explorer	11	3
Total	64	21

It is important to note here that, the research work also employed exclusive criteria to exclude some keywords that are not relevance to the study, and introduced inclusive criteria to narrow the research to the topics that gave useful information to the objective of this paper.

4 Results and Discussion

The selected papers were carefully reviewed and the results of the security issues in the use of mobile educational apps were generated and presented accordingly. This section of the paper presents results on the areas of the security challenges in the use of mobile educational apps, and the way forward or ways to guide against these security challenges in other to maximize the benefit of mobile educational apps. The results are presented in table 4, table 5 and table 6 below:

Table 5. Studies on Security Issues in the Use of Mobile Educational App

Security issues in the use of mobile educational apps	Frequencies of studies	Percentage
Mobile educational apps	10	47%
Security issues	6	28%
Mobile apps	5	23%
Mobile device	4	17.6%

Table 6. The extents of security challenges in the use of mobile educational apps

The extents of security challenges in the use of mobile educational apps	Frequencies of studies	Percentage
Encouraging	15	71.43%
Discouraging	06	28.57%

Table 7. Problems facing the use of mobile educational app in the field of learning

Problems facing the use of mobile educational app in the field of learning	Frequencies of studies	Percentage
Ignorance	11	28.9%
Hackers	3	7.8%
Lack of technical know how	9	23.6%
Lack of adequate power Supply and fund	4	10.5%

5 Discussion

The key for effective use of any mobile applications or technologies in life is to understand the strength and weakness of such an app or technology, especially while deploying it to achieve specific learning goals. Thus, taking the security features of the apps in turn, we realize that 'limiting unauthorized access and learning content security' are useful to the students because of its file-lock and password mechanism which are related to some area in computer security syllabus. More so 'avoiding malware' by the use of antivirus, and 'Free Wi-Fi' unless secured, is another useful part, because this is where people fall victim the more to hacker or the third party. These are some of the best practices that a mobile user must follow in order to have a fully secure difficulty to crack application. However, it should be noted from this study that in the near future, security will act as one of the differentiating and

competing determinants in the app world with customers preferring secure apps to maintain privacy of their data over other mobile applications.

From a critical out look at the way forward of guiding against security challenges in the use of mobile apps, some recommendations and suggestions on improving the apps are as follow: i) Modern biometric security features may be incorporated into the app such as finger prints and voice recognition instead of convectional file lockers and passwords mechanism; ii) Addition of more security notification alerts to other sections of the app aside the unusual behavior section, iii) To include prompt notification alert to Bluetooth and Wi-Fi sections if possible, rather than scanning fully before alert; iv) Security issues on copyright materials can be included in future. That is copyrighted soft copy should not be shared without the author's permission, in form of DRM; v) The app should distinguish real malware from other process and memory intensive app; vi) The developers should keep updating the app in line with future security threats. These recommendations will be considered in the future releases of the app

6 Conclusion

There is evidence that hackers nowadays are targeting mobile applications to gain access over consumer personal information and details, and maliciously use it. Hence, apps developers need to be extra cautious while they build an app for both iOS and android devices. More so, it is necessary for mobile apps developer not to only look at providing new and more features to the customers but also the security aspect of the application, and a source of enlightenment to the users of mobile apps on how to maximize the benefit of mobile educational apps.

7 References

[1] Adedoja, G., Botha, A., & Ogunleye, O. S. (May, 2012). The future of mobile learning in the Nigerian education system. IST-Africa 2012 Conference Proceedings. 9 (11): 34-46.

[2] Agbatogun, A. O. (2013). Interactive digital technologies' use in Southwest Nigerian Universities. Conference for Educational Technology Research and Development. Retrieved 4th May, 2019, http//wwwakpanagbtogun.org https://doi.org/10.1007/s11423-012-9282-1

[3] Batista, S. C. F., & Barcelos, G. T. (2014). Considerations on the use of mobile phones in educational context. International Journal on New Trends in Education and their Implications. 5(1): 1-10.

[4] Brinda, S. & Bala, P. (2017). Privacy risks and security threats in mhealth apps. Journal of International Technology and Information Management. Article 5. 26 (4): 126-153

[5] Gbenga, A. (2006). Information and communication technology and web mining techniques. Paper presented at the education trust fund capacity building workshop for knowledge-driven growth for Nigerian universities, University of Ilorin, Nigeria.

[6] Hinze, A., Vanderschantz, N., Timpany, C., Cunningham, S. J., Saravani, S., & Clive, W. (2017). Use of mobile apps for teaching and research. Retrieved 5th May, 2019, https://doi.org/10.1007/978-3-319-70232-2_15

[7] Hussein, I., Hussain, A., Mkpojiogu, E.O.C., & Nathan, S.S. (2019). The state of user experience design practice in Malaysia. International Journal of Innovative Technology and Exploring Engineering, 8(8S): 491-497.
[8] Hussain, A., Hussein, I., Mkpojiogu, E.O.C., & Sarlan, A. (2019). The state of user experience design (UXD) practice in Malaysia: an in-situ interview approach. International Journal of Innovative Technology and Exploring Engineering, 8(8S): 498-505.
[9] Hussain, A., & Mkpojiogu, E.O.C. (2017). Predicting the perceived worth of software products requirements with customer satisfaction. Advanced Science Letters. 23(5): 4269-4273. https://doi.org/10.1166/asl.2017.8245
[10] Hussain, A., Mkpojiogu, E.O.C., & Nawi, M.N.M. (2017). Capturing customer satisfaction and dissatisfaction in software requirements elicitation for features in proposed software systems. Journal of Engineering and Applied Sciences (JEAS), 12(21): 5590-5597.
[11] Hussain, A., Mkpojiogu, E.O.C. & Yusof, M.M. (2016). Perceived usefulness, perceived ease of use, and perceived enjoyment as drivers for the user acceptance of interactive mobile maps. Proceedings of the 1st International Conference on Applied Science and Technology (ICAST'16), Kedah, Malaysia. AIP Conf. Proc. 1761(1): 020051, https://doi.org/10.1063/1.4960891
[12] Indrajeet, M. K. (February 2016). Security ads in mobile apps. International Journal of Engineering Research and Application. 6 (2): 1-4.
[13] Jayaprakash, S. & Chandar, V. (n. d.). (2019). Use of educational apps in today's classroom. http//www JayaprakashChandar.org
[14] Jegede, P. O. (2009). Age and ICT-related behaviours of higher education teachers in Nigeria. Issues in Informing Science and Information Technology. Retrieved 24th May, 2019, http//www Paulskyjegede.ng https://doi.org/10.28945/1096
[15] Kneil-Boxley, S. (2012). Towards a mobile learning strategy to support Higher Education. Conference for Innovative Practice in Higher Education. Retrieved 24th May, 2019, http//www Boxleykneil.org.ng
[16] LIVA BRAN (n.d.). (2019). The challenges for mobile learning in the classroom and how to overcome them. Retrieved 24th May, 2019, http//www. Lovabran.org.ng
[17] Machado, J. L. A. (2012). Celular na escola: o que fazer? Retrieved 5th May, 2019,
[18] http://cmais.com.br/educacao/celular-na-escola-o-que-fazer. In Batista, S. C. F., & Barcelos, G. T. (2014). Considerations on the use of mobile phones in educational context. International Journal on New Trends in Education and their Implications, 5 (1): 1-10
[19] Osang, B. F., Ngole, J. & Tsuma, C. (2013). Prospects and Challenges of Mobile Learning Implementation in Nigeria: Case Study National Open University of Nigeria (noun)'. A paper presented at International Conference on ICT for Africa 2013, February 20-23, Harare, Zimbabwe.
[20] Oyelere, S. S., Paliktzoglou, V., & Suhonen, J. (2016). M-learning in Nigerian higher education: an experimental study with Edmodo. International Journal of Social Media and Interactive Learning Environments, 4 (1): 43–62. https://doi.org/10.1504/ijsmile.2016.075055
[21] Prashant, K. J., Arnab, G. & Shashikant, R. (2013). Bring your own device (BYOD): security risks and mitigating strategies. Journal of Global Research in Computer Science, 4 (4): 12-17.
[22] Priyanka, G., Sahil, B., & Ajit, S. (November, 2010). A literature review of security attack in a mobile ad-hoc networks. International Journal of Computer Applications, 9 (12): 78-90.

[23] Shabnam, K. K. & Mazleena, S. (2015). Towards the security issues in mobile ad hoc networks. International Journal of Innovative Research in Information Security (IJIRIS), 2 (1): 22-27.
[24] Shaibu, A. S. & Mike, J. (2016). Enhancing mobile learning security. International Journal on Integrating Technology in Education (IJITE). 5(3): 1-15.
[25] Stallings, W., & Brown, L. (2012) Computer Security Principles and Practice (2nd Ed). Prentice Hall NJ: Pearson Education Inc.
[26] UNESCO (2013). Policy guidelines for mobile learning [Guidelines]. Paris, France. Retrieved 5th May, 2019, from http://unesdoc.unesco.org/images/0021/002196/219641e.p
[27] Galina Volkovitckaia, Yuliya Tikhonova, Olga Kolosova. (2020). Educational Experience in the Mobile Learning Environment: Consumer Behavior Perspective. International Journal of Interactive Mobile Technologies. 14(21): 92-106. https://doi.org/10.3991/ijim.v14i21.18441
[28] Korlan Zhampeissova, Irina Kosareva, Uliana Borisova. (2020). Collaborative Mobile Learning with Smartphones in Higher Education. International Journal of Interactive Mobile Technologies. 14(21): 4-18. https://doi.org/10.3991/ijim.v14i21.18461
[29] Ahlam Mohammed Al-Abdullatif, Azza Ali Gameil. (2020). Exploring Students' Knowledge and Practice of Digital Citizenship in Higher Education. International Journal of Emerging Technologies in Learning. 15(19): 122-142. https://doi.org/10.3991/ijet.v15i19.15611

8 Authors

Emmanuel O.C. Mkpojiogu is a Lecturer at Department of Computer and Information Technology, Veritas University, Abuja, Nigeria. Currently, he is a PhD student at School of Computing, Universiti Utara Malaysia. The research area is User Experience, Human Computer Interaction and Software Engineering. He has published many articles in reputable Scopus indexed journals. emmanuel10178@yandex.com

Azham Hussain is the Associate Professor of Software Engineering at School of Computing, Universiti Utara Malaysia, Kedah, Malaysia. He is the founder of Human-Centered Computing Research Group, which is affiliated with the Software Technology Research Platform Center at School of Computing, Universiti Utara Malaysia. Azham Hussain is a member of the US-based Institute of Electrical and Electronic Engineers (IEEE), and actively involved in both IEEE Communications and IEEE Computer societies. azham.h@uum.edu.my

Monday Onah Agbudu is an upcoming researcher with Department of Science Education, Faculty of Education, Veritas University, Abuja, Nigeria. mongenby10@gmail.com

Article submitted 2020-11-27. Resubmitted 2021-01-17. Final acceptance 2021-01-18. Final version published as submitted by the authors.