Mobile Learning Security Concerns from University Students' Perspectives

Shaibu Adekunle Shonola
Department of Computer Science
University of Warwick
Coventry, United Kingdom

Mike S Joy
Department of Computer Science
University of Warwick
Coventry, United Kingdom

Abstract

The use of mobile devices as learning aids is increasing due to availability and affordability of mobile phones, smartphones and tablets among students. Many learners use their handheld devices not only for calling and texting, but also for educational purposes. Some promoters and developers of mobile learning in universities are developing and delivering learning content and instructions on mobile devices without adequate consideration for security of stakeholders' data, whereas the use of these mobile technologies for learning poses a serious threat to confidentiality, integrity and privacy of those involved in learning delivery, including the students. This paper discusses the security concerns of mobile learning from the learner's perspective based on a study conducted in higher education institutions in Nigeria. The study identified the security threats that learners may face when using mobile devices for educational purposes and examined the perceived damaging effects of mobile learning on students in cases there is a security breach. This paper concludes with recommendations for alleviating the security threats.

***Keywords**: mobile learning, m-learning, m-learning security, security issues, security concerns, mobile device.*

I. INTRODUCTION

The main focal points of m-learning are using the exponential growth in mobile technologies to the greatest advantage of the students to complement their learning process and to shorten the learning curve [1]. Another reason for m-learning is information sharing, which makes is possible for learners to interact with each other and share knowledge anytime. Mobile phones are generally used by students to access course material and learning instruction [2] and many learners already explore the interactivity and sociability of web 2.0 technologies, such as wikis, online forums, blogs, image sharing and other social media, especially in the area of arts and humanities [3].

One of the advantages of mobile learning is that it gives learners a certain amount of freedom and independence in their course of learning [4]. It also allows students to communicate with their lecturers and get information from them while on the move. Thus, students who use mobile technologies for learning are not far from their lecturers and tutors, they are also in full control accessing learning content and instructions on their mobile devices. The study conducted by Taleb and Sohrabi in [5] showed that students who use mobile devices in their courses are more motivated to learn than those who do not use their mobile devices for learning.

However, the use of mobile technologies by students has some security effects in term of integrity, confidentiality, and privacy of the users [6]. Students' records, e-portfolio data, assessment results and feedback are some examples of information that need to be safeguarded when using mobile devices in education. Therefore, the security challenge is to ensure that students' have access only to their required learning material and instruction regardless of whether they learnt in the lecture room or outside the classroom [7]. While these challenges affect the use of mobile learning in Higher Education Institutions (HEI) and the students' viewpoints on mobile devices for learning in general, this paper specifically examines Nigerian students' perspectives on security issues that affect m-learning.

The first part of this paper is a review of related work on m-learning and security issues around it. It reviews various studies on m-learning security and evaluates the recommendations made in the literature. The second part deliberates on the research carried out on security issues that affect the use of mobile learning from Nigerian university students' perspectives, and details - the purpose of the research, the methodology and the research questions. A brief outline of the analysis of the results of the research is presented in section three of the paper while section four gives a detailed discussion on the results obtained. The final part of the paper summarises the results and discusses recommendations to address the security issues mentioned in the earlier sections. The paper concludes with problems encountered during the research and directions for future work in ensuring a robust and highly secure mobile learning environment for students in HEIs most especially in Nigerian universities.

978-1-4799-4743-0/14/$31.00 ©2014 IEEE November 13-14, 2014, Thessaloniki, Greece
2014 International Conference on Interactive Mobile Communication Technologies and Learning

II. LITERATURE REVIEW

Mobile devices facilitate innovative ways for students by enhancing their learning experience through m-learning. Like any other technology, mobile devices are prone to security risks. The security issues inherent in mobile devices are also transferable to the m-learning context. Some perceived risks in m-learning include unauthorised interfering with the learning content and instructions by the learners. Educators and Higher Educational Institutions are concerned about the increasing threats to users' data security and privacy. More importantly learners are allowed to use their portable devices to access learning content and materials anywhere, thus increasing the security risks. Some notable works on mobile learning and learners' experience are evaluated below.

Some researcher scholars, Zamzuri *et al.* [8] observe that students, being stakeholders in the educational environment, use electronic learning system and they are concerned about their privacy and security when using the system. The authors state that students are worried that confidential information such as their assessment grades and feedback might be exposed to their colleagues and they propose that students' needs and views should be given adequate consideration during implementation of m-learning. Alwi and Ip-Shing [9] studied students' perceptions of an e-learning system (m-learning is a subset of e-learning) and discovered that there are security issues in the e-learning systems and they concluded that reliability in an e-learning system is important in securing patronage for the modern learning environment. While these two studies highlights confidentiality and privacy as issues in m-learning, they did not discuss in details these security issues and failed to mention other security risks students encountered when using their mobile devices for learning purposes.

Boyinbode and Akinyede [10] argue that m-learning is the access point to e-learning for many undergraduate students in Nigeria and that it is playing an important role in e-learning by bringing e-learning to students in rural communities. Adedoja *et al.* [11] observe that students are able to send and receive learning content that contains text, graphs, images and video making it a platform to create reality and dynamism for effective learning. The authors observe that mobile devices improve the productivity and efficiency of learners in Nigeria by delivering educational materials and support in real time and in the right context for their immediate needs, and they conclude that having a good mobile technology infrastructure, and since there are no other alternatives, mobile learning is a good choice for Nigerian students. Furthermore, the study by Rafiu *et al.* [12] shows that students in Nigerian universities were well prepared and ready for m-learning as they have various types of mobile devices in their possession and demonstrated high level usage skills for successful application of m-learning in Nigeria.

A study conducted recently by Osang *et al*. [13], however, identifies the adverse effects of social media on mobile learning which include joining negative groups on social networks by the students. This may threaten their personal safety and the security of their handheld devices. The authors highlight the severe dangers unassuming people are exposed to in the hands of those who misuse mobile technology such as identity theft and loss of privacy. Another study conducted in Malaysia by Alzaza and Yaakub [14] shows that students have adequate knowledge and good awareness in the use of mobile technology for their educational needs. While the studies examined above are significant because they discuss students' views on mobile learning and security systems, they do not mention in detail security challenges that students are facing when using their mobile devices for learning purposes.

This paper, will therefore examine mobile learning security from the students' perspectives. This study will investigate learners' concerns on security issues that might affect m-learning in Higher Education Institutions in Nigeria, the damaging effects of m-learning security issues to the students in case of a security breach as well as the strategies for alleviating these security issues.

A. RESEARCH QUESTIONS

The purpose of this study is to provide answers to the following questions.

(1) How important students consider the security of their mobile devices?
(2) What risks and security issues may students have when using their mobile device for learning?
(3) What are the damaging effects of m-learning security risks to the students?

III. METHODOLOGY

A survey research approach was adopted using a sample population of computer science students in their final year of their study was conducted as a data source. A set of questionnaires was delivered to 125 randomly selected students in three Higher Education Institutions in Nigeria. The questionnaire comprised 21 single and multiple choice questions divided into 4 parts. Part one was on demography to collect personal information from the participants. Part two collected data about various mobile devices used by the respondents and the type of activities they were being used for. Part three gathered data on students' awareness on mobile learning and learning activities their mobile devices were being used for in order to determine if m-learning

improved their learning skills and performance. Part four was based on security aspects of m-learning. The questionnaire concluded with an assessment of how mobile learning security issues can be assessed and reduced. A pilot survey was carried out within a small group of participants who were asked to review the questionnaire. Their opinions and suggestions were taken into consideration in making the final version of the survey. The paper-based instruments were distributed after core lectures during the first semester of the 2013/2014 session while a link to the online version was given to the participants to complete at their discretion. Ethical consent was sought and obtained for the study through the authors' university and participants of the survey were assured anonymity. 120 questionnaires were returned back, the data were analysed and presented using frequency distributions, histograms, pie charts and statistical tests.

IV. RESULTS

Table 1 shows a breakdown of the trial participants by gender and age. The findings of this work are organised into three sections in order to provide answers to the research questions as shown below:

Table 1: Participant Demographics

Gender	Frequency	Percentage (%)
Female	63	52.5
Male	57	47.5

A. Research Question 1: How important students consider the security of their mobile devices?

This research question is to determine how important the students consider the security and safety of their handheld devices -- mobile phones, smart phones, tablets and other handheld devices they used for learning purposes. It is a single choice question and all the 120 students responded. Using the gender distribution, 69.84% of the female and 71.93% of the male students indicated that their mobile devices are very important to them. 28.57% of the female and 24.56% of the male responded that their mobile devices are important to them as shown in fig 1.

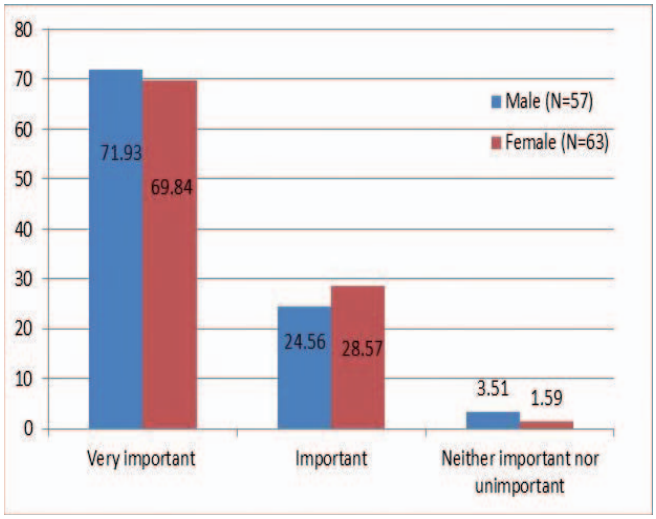

Fig. 1: How important students consider the security of their mobile devices

The various reasons why the security of m-learning devices is important to the students are highlighted in the discussion section of this paper.

B. Research Question 2: What risk and security issues may students have when using their mobile device learning?

The research question is a multi-choice question to find out various security issues respondents might have encountered when using mobile devices for learning activities. 65.08% of the female and 59.65% of the male indicated theft or loss of device, 60.31% of the female and 70.18% of the male indicated that colleagues and friends have used their handheld device without their permission. 74.6% of the female and 75.44% of the male responded that virus or malware attack is a concern to them while 25.4% of the female and 33.33% of the male noted denial of service.

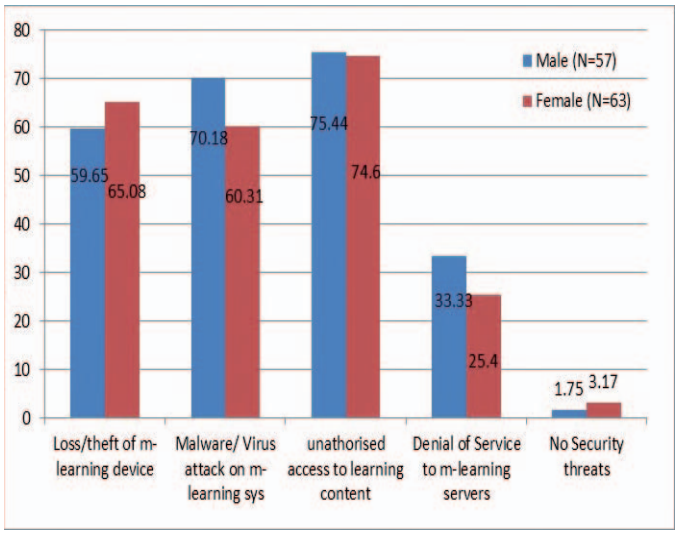

Fig. 2: Security issues learners may encounter in m-learning

C. *Research Question 3: What are the damaging effects of m-learning security threats to the students?*

The most common effect of m-learning security to students in HEIs in Nigeria is loss of confidential or personal information as perceived by 85.71% of the female and 73.68% of the male. A large numbers, 71.43% of the female and 71.93% of the male respondents feared loss of study hours as the effect of security threat. Similarly, 60.32% of the female and 70.18% of the male participants perceived loss of performance as security risks. Psychological effects resulting from security breaches of mobile devices account for 47.62% of the female and 45.61% of the male students' responses.

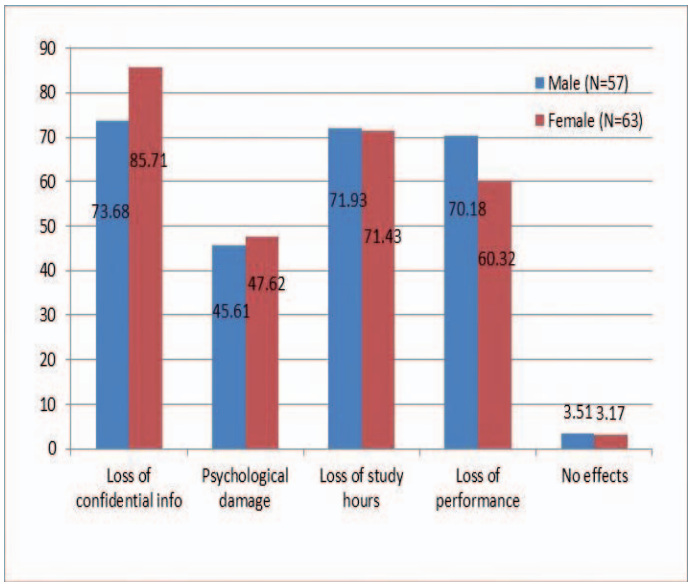

Fig. 3: Damaging effects of m-learning security threats to students

V. STATISTICAL TESTS ANALYSES

The results obtained were further analysed using the chi-square statistical test and Mann- Whitney U test for dependency based on gender differences. The chi-square test was first carried out to determine the importance of the security of mobile devices to the students. The chi-square statistic was calculated as 0.6408, P-Value as 0.725852 at the confidence interval of 0.05. The test shows that there is no gender difference on how important the students consider the security of their m-learning devices.

The second research question on the risk and security issues that students may have when using their mobile devices for learning, Mann- Whitney U test was used for the calculation as shown in table 1 and table 2 below.

Table 1: Ranking of female and male on m-learning security

Gender	Participants	mean of ranks	sum of ranks
Female	63	5.8	29
Male	57	5.2	26
Total	120	5.5	55

Table 2: Mann- Whitney test

Test	m-learning security threats
U Mann-Whitney	11
Z	0.2089
Sig (2-tailed)	0.83366

According to the table 2, there is no significant difference between female and male students' viewpoints in relation to the security threats in m-learning. This implies that there is no gender difference on the perceived risks of m-learning devices and that both male and female observe similar security risks.

Furthermore, Mann- Whitney U test was also used for the statistical analysis of perceived damaging effects of security risks as shown in table 3 and table 4 below

Table 3: Ranking of female and male on m-learning security

Gender	Participants	mean of ranks	sum of ranks
Female	63	5.9	29.5
Male	57	5.1	25.5
Total	120	5.5	55

Table 4: Mann- Whitney test

Test	m-learning effects
U Mann-Whitney	10.5
Z	0.3133
Sig (2-tailed)	0.75656

According to the table 4, there is no gender difference in the perceived damaging effects of security breach to the students. This implies that both the male and female students perceive the same damaging effects on m-learning security risks.

VI. DISCUSSION

Fig. 1 shows how important students take the security of their mobile devices. Most of the 120 respondents said that the security of their mobile devices is important to them. This study confirms that many students take the security of their mobile devices seriously and this is expected considering the usefulness of handheld devices in day to day activities as every student carries at least one mobile device.

Some of reasons given by the students for taken the security of their mobile device very important are as follows

- Mobile phones and smartphones are considered to be valuable personal property among the students, thus they try as much as possible to keep them safe.
- Many learners use their handheld devices to exchange education-related messages and learning contents with classmates, search the internet and library databases for learning materials, and hold group discussions with classmates. Therefore, they believe that their mobile device is vital to their academic success and are mindful about its security and safety.
- Furthermore, many students also use their handheld device as data storage, thus they have their personal information on their mobile devices, and so having security awareness is an important aspect of protecting their privacy. The result is supported by the work of the author in Kambourakis [15] that discusses the security and privacy challenges of m-learning and suggests that learners are extremely concerned about the security and safety of their data stored on mobile devices.

Fig. 2 illustrates security issues students may encounter when using mobile devices for learning. Conspicuous in the list is loss or theft of mobile devices. This bad habit is common in many developing countries since mobile devices are still regarded as precious possessions and in some cases where the Higher Educational Institution supplies learners with mobile devices, there are concerns about making learners attractive to thieves. This result is in line with the work of Obodoeze *et al*. [16] which identifies that the second most challenging security concerns affecting mobile users in Nigeria is the frequent or widespread losses of mobile device by their owners to thieves at gunpoint or the owners negligently lose their mobile phones while in transit. It is also consistent with a survey conducted by Jupiter [17] on mobile device users that showed that one out of every three mobile device users has lost their device at some point in time.

Virus and malware attack is also a threat to the use of handheld devices for learning purposes. This study also supports the work of Obodoeze *et al*. [16] who identify the various forms of threats including virus/malware attack and hacking as the biggest security challenges being faced by mobile device users in Nigeria. Virus and malware threats are normally encountered when downloading educational materials from an unknown source. Similarly, unauthorised use of portable devices by friends or classmates of the owners is also common. This behaviour is rampant among learners in Nigeria as they usually live in shared hostels. Mobile devices left on a table can be picked by roommates and use for gaming or educational purposes which can lead to unauthorised access to confidential information of the owners since many students have their details such as full name, address, date of birth, email address and even their bank account information on apps on their mobile devices.

Denial of service is also a threat that many students are concerned about and usually affects the availability of m-learning system. It is a threat that results from irregular power supply to mobile learning servers, a problem that is common in developing countries. This study is also consistent with the results of a study of Osang *et al.* [13] in which 64% of the respondents identify that the poor power supply situation in the country is a barrier to mobile learning. Denial of service can occur during scheduled or unscheduled downtime due to maintenance of network infrastructure which can lead to loss of connectivity between mobile devices and servers. It can also be caused by physical attacks on network infrastructure on university campuses which are common, for example during student riots in some universities in developing countries such as Nigeria.

Furthermore, denial of service can be caused by illegal activities of hackers either by shutting down services intentionally or deletion of valuable files to deprive users the services of a resource they would normally expect to have. It is aimed at complete disruption of the whole operation of wireless network and normally affects the availability of m-learning system. However, it is observed that the security threats – theft of mobile device, virus/malware attack, unauthorised access and denial of service issues as perceived by the learners, are not specific to them alone. These are general problems relating to the use of mobile devices either for learning or otherwise, considering the fact that in developed and developing countries virtually every young people carries at least one mobile device.

Fig. 3 illustrates the damaging effects to the students if a security breach occurs. A very high percentage of the learners agreed that loss of confidential information is the most harmful effect. This result is consistent with the work of Zamzuri *et al*. [8] which states that one of the reasons why students reject online systems is due to security reasons because they are worried about the loss of their private and confidential information. The study further revealed that at least 60% of the students feared loss of study hours and performance as consequences of a security breach in m-learning due to denial of service. This is possible when learners have viewed m-learning as a complement to classroom and relied on it as a learning portal. Thus the non-availability of service for a long period of time will have adverse effects on learners' study hours, revision time and consequently their performance. This finding is in line with the work of Kukulska-Hulme *et al.* [18] which shows that good m-learning improves learners' study retention and performances in their study. Therefore, learners need a reliable, highly available and dependable m-learning system

to avoid being frustrated when using the system that can influence their study performance.

Some of the learners (47.62% of the female and 45.61% of the male) indicated that they are likely to experience physiological disturbance if their personal information is leaked through a mobile device or m-learning system or if their privacy is infringed. However, 3.33% of the learners stated that a security loophole in an m-learning system poses no adverse effect to them because they have security awareness about the information they have on the mobile devices and they avoid as much as possible storing private information on their mobile devices.

VII. SECURITY RECOMMENDATIONS FOR STUDENTS

Having discussed the issues pertaining to m-learning security as well as the damaging effects from learners' viewpoints, it is important to highlight possible recommendations and put in place strategies for alleviating these security issues in mobile learning systems, starting from the mobile devices and including the servers and network infrastructure. In view of the students concerns on m-learning, the following recommendations are offered for secure and effective m-learning.

- M-learning developers and administrators should create security awareness and education on mobile security among students and encourage them to be security conscious when using their mobile devices. Creating security awareness is vital as our study revealed that some users do not take the security of their mobile devices very seriously and there is a need to promote mobile security education among users [19]. With adequate knowledge, students will be more security conscious about the safety of their handheld devices. Being security conscious will make learners take proper care for their devices and it will invariably solve one of the issues raised by the learners, which is the rate at which the devices are lost or stolen. Since 65.08% of the female and 59.65% of the male respondents' indicated theft or loss of the device, this suggests that educating the learners on security will have huge impacts in reducing the rate at which small electronic gadgets are lost or stolen which is mainly due to their negligence.

- Security apps such as phone finders should be installed on mobile devices to enable them to be located in case of lost or theft. Remote wipe apps should be installed to prevent unauthorised access to confidential and private information as well as learning materials stored on the devices if a lost device cannot be traced.

- Students should avoid connecting to unsecured public Wi-Fi as many of them connect to educational resources while on the move using any free available Wi-Fi. They should be aware of the credibility of the organisation providing the connection regarding the security and safety of free network facilitates before using it. For example, connecting to an unsecured and unverified wireless infrastructure increases the chances of putting personal data at risk. Therefore, learners should be aware of the potential risk of automatically connecting to unknown free wireless access points, which may be intercepted or controlled by attackers and may lead to unauthorised access to their mobile device and learning materials in it.

- Unauthorised access to learning materials can be reduced by having robust access control mechanisms for authentication and authorisation before permission is given to access the device or view learning content and materials. Password lock or biometric access will prevent other learners from using the device if left on the table by the owner. Meanwhile, mobile devices should not be left on the table unattended if the owner is security conscious as mentioned earlier. Devices like mobile or smart phones should remain in owners' pockets when not in use while tablets should be locked away. Similarly, encryption of data on m-learning devices will safeguard learning content from unauthorised access if lost or stolen.

- Denial of service to educational resources can be overcome by putting in place proper security procedures and policies that will prevent hacking activities that deny legitimate acts. A scheduled maintenance policy for m-learning servers and network infrastructure, as well as an uninterruptible power supply, can also prevent service denial by providing a constant power supply. DoS resulting from network breach can be avoided using prevention techniques for counteracting DoS such as protocol traceback techniques on the m-learning servers [20] and reverse proxies spread across multiple hosting locations.

- The recommendation for alleviating security issues on virus and malware attacks on m-learning devices is the use of legacy protection mechanisms and it involves having regular data backups, installing firewalls and having up to date anti-malware and anti-virus software installation on m-learning devices. Furthermore, all interfaces including Bluetooth interfaces should be highly

secured. For example, mobile firewalls normally inspect IP interfaces, but they often overlook the Bluetooth interface [21].

VIII. CONCLUSION AND FURTHER RESEARCH AREAS

Students are eager to use their smartphones and other mobile devices for learning not only to complement their classroom lectures, but also to achieve the globalisation objective in education sector [22]. Their interest and skills in using handheld devices are potentials for m-learning if incorporated into their learning activities [23]. However, students are concerned about the security and confidentiality of their private information being exposed in the process of m-learning. Consequently, the universities advocating m-learning must provide robust mechanisms to support authentication, authorisation, content copying and downloading in m-learning system and as well as safeguard students' assessment and feedback processes from attackers and impostors.

Furthermore, e-portfolio data as well as students' records are some of the confidential information that needs to be protected, in addition to personal information that is kept on their mobile device. The safety of their privacy should be guaranteed at all times [24] by ensuring that adequate security measures are maintained when connections are made between the students' mobile devices and m-learning servers through deployment of proper security policies and measures. Students should also ensure that they connect their devices to a trusted and tested public network in order to safeguard data being transferred during the m-learning process and that they do not download learning materials from unknown sites.

This paper presents the position of learners on security aspects of mobile learning based on the research conducted in universities in Nigeria and is a reflection of their understanding on security issues mobile learning. It was observed that responses of the participants were based on their experience and their knowledge about m-learning security issues. Therefore, some of the responses given by the students to the question may relatively subjective to their theoretical knowledge rather than individual experience with m-learning systems. However, the results of this survey are reliable and consistent with other similar studies in the field as cited above and they are applicable to m-learning in HEIs around the world.

Mobile learning patronage is increasing as technology develops, invariably the security issues in mobile devices are also on the increase and they are transferable to m-learning systems. Students who are the main users of m-learning are most highly likely to be affected by the security threats. Therefore, adequate security education and awareness in a form of tutorials and tips should be put in place for the students in order to minimise their exposures to security issues.

Extensive work has been done on some areas of m-learning security such as security frameworks for mobile learning environments [25] and mobile learning security issues from lecturers' perspectives [26], but there are still many grey areas on m-learning security where little or no research has been done such as attack vectors in m-learning systems, the common ways of breaching m-learning security, collective responsibilities of m-learning stakeholders and other perceived threats to m-learning in developing countries apart from security. Therefore, future research work can focus on these grey areas.

REFERENCES

[1] D. Keegan "The incorporation of mobile learning into mainstream education and training". World Conference on Mobile Learning, Cape Town, pp. 11, October 2005.

[2] R. A Aderinoye, K. O Ojokheta and A. A Olojede "Integrating mobile learning into nomadic education programmes in Nigeria: issues and perspectives, international Review of Research in Open and Distance Learning" vol.8, no.2, pp. 44-52, 2007

[3] C.Greenhow, B. Robelia and J.E Hughes "Learning, teaching, and scholarship in a digital age Web2.0 and classroom research: what path should we take now?" Educational Researcher, vol.38, no.4, pp.246–259, 2009

[4] M. O. M El-Hussein and J. C. Cronje "Defining mobile learning in the higher education landscape " Educational Technology & Society, vol.13, no.3, pp.12–21, 2010

[5] Z.Taleb and A. Sohrabi "Learning on the move: the use of mobile technology to support learning for University Students" International Conference on Education & Educational Psychology, Procedia Social and Science Behaviour. vol.69, pp. 1102 – 1109, December, 2012

[6] A. Charlesworth "Code of practice for the further and higher education sectors on the data protection act 1998", Tech. rep., JISC Legal, (2009), Available online from http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/ DPACodeofpractice.pdf. [Accessed on June 12, 2013]

[7] F. Graf "Providing security for elearning". Computers & Graphics. vol.26, no.2, pp.355–365, April, 2002

[8] Z. F. Zamzuri, M. Manaf, Y. Yunus and A. Ahmad "Student perception on security requirement of e-learning services" 6th International Conference on University Learning and Teaching Procedia-Social and Behavioral Sciences. Vol.90, pp.923-930, October, 2013

[9] N. M Alwi and F. Ip-Shing "User's perception in information security threats in E-learning" A paper presented at the 2nd International Conference of Education, Research and Innovation. ICERI2009 Proceedings, Madrid, Spain. pp. 2345-2352, November, 2009

[10] O. K Boyinbode and R. O Akinyede "Mobile learning: an application of mobile and wireless technologies in Nigerian learning system" International Journal of Computer Science and Network Security (IJCSNS) vol.8, no.11, November 2008.

[11] G. Adedoja, A. Botha, and O. S Ogunleye "The future of mobile learning in the Nigerian education system" IST-Africa 2012 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2012.

[12] M. I Rafiu, S. A. Kayode and T. O.Rapheal "Implementing mobile e-learning in Nigeria tertiary educational system – A Feasibility Study"

International Journal of Science and Advanced Technology, vol1 no.1,pp. 7, 2011

[13] F. B Osang, J. Ngole, C. Tsuma "Prospects and challenges of mobile learning implementation in Nigeria case study National Open University of Nigeria NOUN" International Conference on ICT for Africa 2013.February 20-23, 2013 Harare Zimbabwe

[14] N. S Alzaza and A. R Yaakub "Students' awareness and requirements of mobile learning services in the higher education environment" American Journal of Economics and Business Administration vol.3, no1, pp. 95-100, 2011

[15] G. Kambourakis "Security and privacy in m-learning and beyond: challenges and state of the art" International Journal of u- and e-services" Science and Technology, vol.6, no.3, June, 2013.

[16] F. C. Obodoeze, F. A Okoye, C. N. Mba, S. C. Asogwa and F. E.Ozioko "A holistic mobile security framework for Nigeria" International Journal of Innovative Technology an Exploring Engineering (IJITEE), vol. 2, no. 3, pp.1-11, February, 2013

[17] Juniper Networks "2011 Mobile threats report" Juniper Networks Inc, February, 2012

[18] A. Kukulska-Hulme, M. Sharples, M. Milrad, I. Arnedillo-Sánchez and G. Vavoula "Innovation in mobile learning: a European perspective." International Journal of Mobile and Blended Learning, vol.1, no.1, pp.13-35, 2009

[19] S. Diaz, "Mobile security needs more than just software, needs education," July 1, 2010, Available online from http://www.zdnet.com/blog/btl/mobile-security-needs-more-than-just-software-needseducation/36437 [Accessed on Jan 20, 2012].

[20] U. Tupakula and V. Varadharajan (2013). 'Security Techniques for Counteracting Attacks in Mobile Healthcare Services'. The 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2013). Procedia Computer Science, vol. 21, pp. 374 – 81

[21] A. Razaque, A and K. Elleithy "Discovery of malicious attacks to improve mobile collaborative learning (MCL)" International Journal of Computer Networks & Communications (IJCNC)", vol.4, no.4, 2012

[22] M. Hashemi, M. Azizinezhad, V. Najafi and A. J. Nesari "What is mobile learning? challenges and capabilities" 2nd World Conference on Psychology, Counselling and Guidance 2011, Procedia Social and Science Behaviour, vol. 30, pp. 2477 – 2481, December, 2011

[23] C. Dale and G. Povey "An evaluation of learner-generated content and podcasting" Journal of Hospitality, Leisure, Sport and Tourism Education [Online] vol. 8, no 1, pp.117-123, 2009

[24] C. D. C. Luminita and C. I. N Magdalen "E-learning security vulnerabilities", 4th World Conference On Educational Sciences February 2012 Barcelona, Spain Procedia - Social and Behavioral Sciences vol. 46, pp. 2297 – 2301, February, 2012

[25] S. A Shonola and M. S. Joy (2014). "Security framework for mobile learning environments" In press (2014).

[26] S. A. Shonola and M. S. Joy "Mobile learning security issues from lecturers' perspectives (Nigerian universities case study)". A paper presented at the 6th International Conference on Education and New Learning Technologies, Barcelona, Spain, 7 – 9 July 2014.