MOBILE LEARNING SECURITY ISSUES FROM LECTURERS' PERSPECTIVES (NIGERIAN UNIVERSITIES CASE STUDY)

Shaibu Adekunle Shonola, Mike Joy

Department of Computer Science, University of Warwick (UNITED KINGDOM)

Abstract

The demand for mobile learning has continued to increase due to recent advances in modern technologies. Mobile learning advocates in universities focus their attention mainly on course development, deployment and delivery on handheld devices but they pay little or no consideration to security and privacy of stakeholders' data in the design of mobile learning systems. However, the use of mobile technologies for learning poses a threat to confidentiality, integrity and privacy of the data involved in learning delivery for both learners and lecturers. This paper discusses the security concerns of mobile learning from the lecturers' perspective based on a study conducted in higher education institutions in Nigeria. While the challenges of adopting mobile learning in Nigerian universities are enormous, the study identifies the critical security challenges that educators are facing when using mobile devices for educational purposes. It further examines the damaging effects of mobile learning on educators if their privacy breached and provides recommendations for alleviating the security threats.

Keywords: mobile learning, m-learning, m-learning security, mobile device, handheld device.

1 INTRODUCTION

The advent of m-learning is creating a new environment for teaching, learning and group discussion. It allows learners to communicate with lecturers and peers, as well as access learning content and resources, while on the move. Examinations and assessments can be done via mobile devices and feedback can be received through them. Lecturers can give out lecture notes and instructions while on the move and students can listen to recorded lectures either online or offline anytime anywhere. M-learning therefore, extends learning beyond lecture theatres and can be made to support modern classroom learning tools [1]. This undoubtedly makes learning an exciting experience for the students and teaching a very interesting career for the lecturers.

However, there are concerns that stem from the use of mobile technology for learning and teaching purposes that may affect m-learning adoption negatively. One of these is the integration of m-learning into classroom teaching without giving extra workload to the lecturers who may be more concern about delivering lectures in the classroom in line with the university curriculum and carrying out their research activities. Mobile learning may give additional responsibility to lecturers in terms of preparation which might entail repackaging course content to fit a variety of mobile devices. The acceptance and readiness to use mobile technology by the lecturer as well as the learners is another critical issue that will determine the success rate of mobile learning implementation [2].

The most important concerns about the use of mobile devices in learning are the security risks and vulnerability attack issues on learning content and private information of stakeholders including the educators [3]. Given their high portability, mobile learning devices such as smartphones and tablets are very susceptible to physical and digital attacks, and they are becoming targets mainly because of their widespread use [4]. The concern about security risks and privacy issues in the m-learning realm seems to be quite high among educators most especially in a developing country like Nigeria where there is a huge amount of cybercrime and internet security threat [5].

The first section of this paper is a review of related work on m-learning security. It summaries existing work on m-learning security and evaluates recommendations made in the literature. The second section discusses the research carried out on security issues that affect adoption of mobile learning in Nigeria from instructors and lecturers perspective, and details the purpose of the research, the methodology and research questions. 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 last part of the paper highlights and discusses recommendations to overcome the security issues mentioned in the previous sections. The paper concludes with problems encountered during the research and direction for future work in ensuring a robust and highly secure mobile learning environment.

ISBN: 978-84-617-0557-3

2 BACKGROUND/RELATED WORK

In as much as mobile devices have capabilities to motivate modern and innovative ways of learning, the security issues inherent in mobile devices are also transferable to m-learning. Whilst mobile devices are much more in use and connected to the outside world than PCs, they have many weak points susceptible to attack and they normally do not come with antivirus or anti-ware software. The basic security requirements to be considered in order to cope with the threats in mobile access are confidentiality, authenticity, mobile data integrity, control and availability and several researchers have noted that privacy issues remain a key concern when individuals confront any security threat.

The author in [3] provides a comprehensive review and classification of literature relevant to security and privacy in the m-learning environment. He further identifies challenges in security and privacy in the m-learning setting most of which are adopted from e-learning systems such as- security and privacy of data and system, safeguarding of data stored on mobile devices, prevention of offensive or illegal behaviour, content filtering, protection of data in the cloud, and protection of copyright. He states that the challenges have to do with securing m-learning systems and deploying suitable security policies and procedures to detect and deter attacks and ensuring the integrity, privacy and confidentiality of the data stored and transferred. While the author provides many insights on mobile learning security and privacy in general, these come mostly from e-learning context in Europe, whereas our paper is based on m-learning security threats from Nigerian universities environments.

The authors in [6] discuss possibilities and challenges of m-learning in Nigerian universities. The challenges they raised on m-learning devices includes small screens, tiny keyboards preventing efficient input, high prices, and limited computing capability and connectivity issues. They further mention the lack of technical experts in the mobile learning field and adaptation of mobile software for the Nigerian educational curriculum as some of the challenges facing m-learning in higher education institutions in Nigeria. The challenges of aligning m-learning in Nigerian National Curriculum were also highlighted by authors in [7]. However, while their research is a significant piece of work on mobile learning in Nigerian Higher Education Institutions, they fail to address security threats as a challenge in Nigerian universities. Furthermore, the latest mobile devices have screens that are big enough and keyboards that are suitable for learning. The newest mobile devices have powerful computing capability while their prices are also falling significantly [8].

In a recent study conducted by [2], 56 out the 80 educators (representing 70.1%) interviewed considered security issues as one of the main barriers to successful implementation of mobile learning in Nigeria. They stated that educational institutions, educators, and learners are extremely concerned about the growing threats to data security and privacy. If lecturers want to go by the security challenge currently facing the country, they will prefer their identities to remain confidential as a preventive measure towards falling target to unsuspecting mischief makers who can use their identity to perpetrate malicious acts. This work is relevant because it discusses the prospects and challenges of mobile learning in Nigeria and their study was carried out in the same geographical location, however, it fails to mention specific security challenges the educators are facing when using mobile devices as teaching aids.

This paper will therefore, determine mobile learning security from the teachers' perception. This study will examine lecturers' 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 lecturers in case of a security breach as well as the strategies for alleviating these security issues.

2.1 Research Questions

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

(a) What are the lecturers' concerns on security issues that might affect m-learning in Higher Education Institutions in Nigeria?

(b) What are the damaging effects of m-learning security issues to the lecturers?

(c) What are strategies for alleviating these security issues?

3 METHODOLOGY

The study employed a survey research approach using a sample population of computer science lecturers and instructors. The data collection method involved interviewing 30 lecturers in Computer

Science departments in three Higher Education Institutions in Nigeria. Students' opinions were also obtained by delivering a set of questionnaires to 90 year three and final year undergraduate students at the same institutions. Before the field study was carried out, a small group of colleagues was asked to review the questionnaire and mock interviews were conducted. Opinions and suggestions given by them were taken into consideration in making the final copy of the survey. A pre-test was conducted for the second time to another group of colleagues in other to ensure high reliability and understanding of the questions.

The paper-based questionnaires were distributed at core lectures during the 2013/2014 session while the online version survey was published on http://www2.warwick.ac.uk/fac/sci/dcs/research/edtech/surveys/securemobilelearning/. Ethical consent was obtained for the survey through the authors' university (BSREC approval REGO-2013-472), and interviewees and respondents to the questionnaire were assured anonymity. Interviews were held with lecturers and instructors in computer departments and the copies of the questionnaire that were administered by the researcher were returned for analysis. The data collected were analysed and presented using frequency distributions, pie charts and histograms.

4 RESULTS

The findings of this work are organised into three sections in order to provide answers to the research questions as shown below:

4.1 Research question 1

What risk and security concerns might lecturers encounter when using mobile devices as teaching aids?

This section addresses security issues lecturers may encounter when using mobile devices as teaching aids. Top on the list is privacy issues and students exploiting a security breach in m-learning system to perpetrate malicious acts, followed by data interception to commit illegal or fraudulent activities.

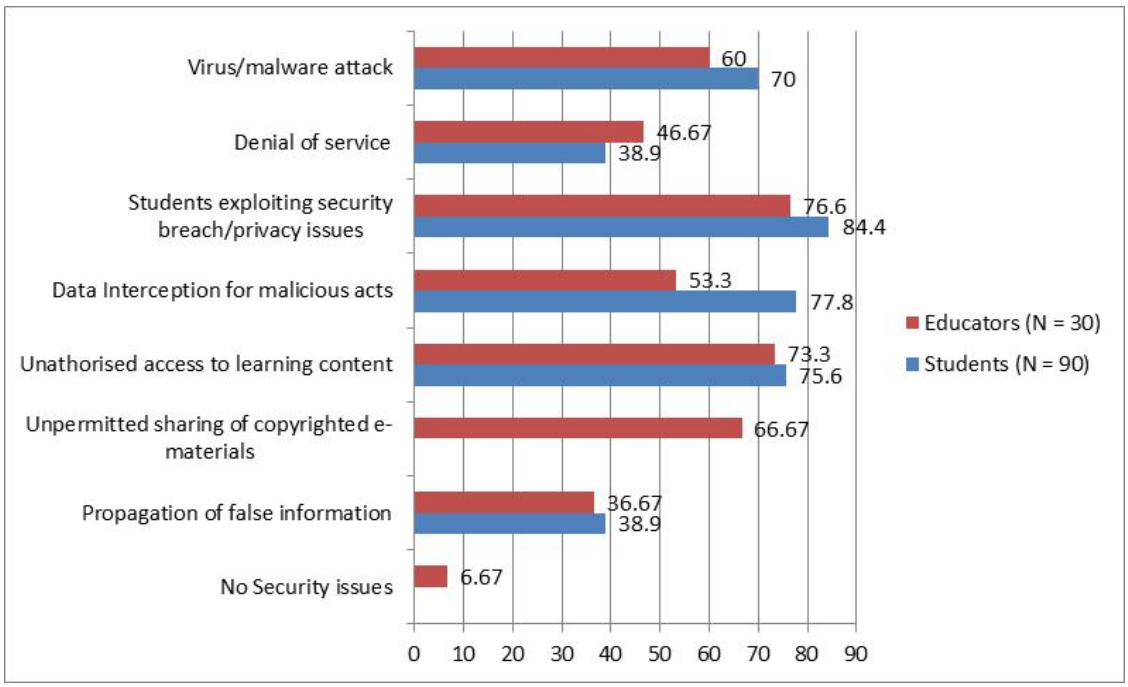

Fig. 1: Security issues lecturers might encounter in m-learning

4.2 Research question 2

What are the adverse effects of m-learning security threats to the lecturers in Nigeria?

The most damaging effect identified in figure 2 is the loss of confidential information. Some educators also believed that unauthorised change of learning content and loss of control during e-examination as the main issues instructors may encounter in m-learning

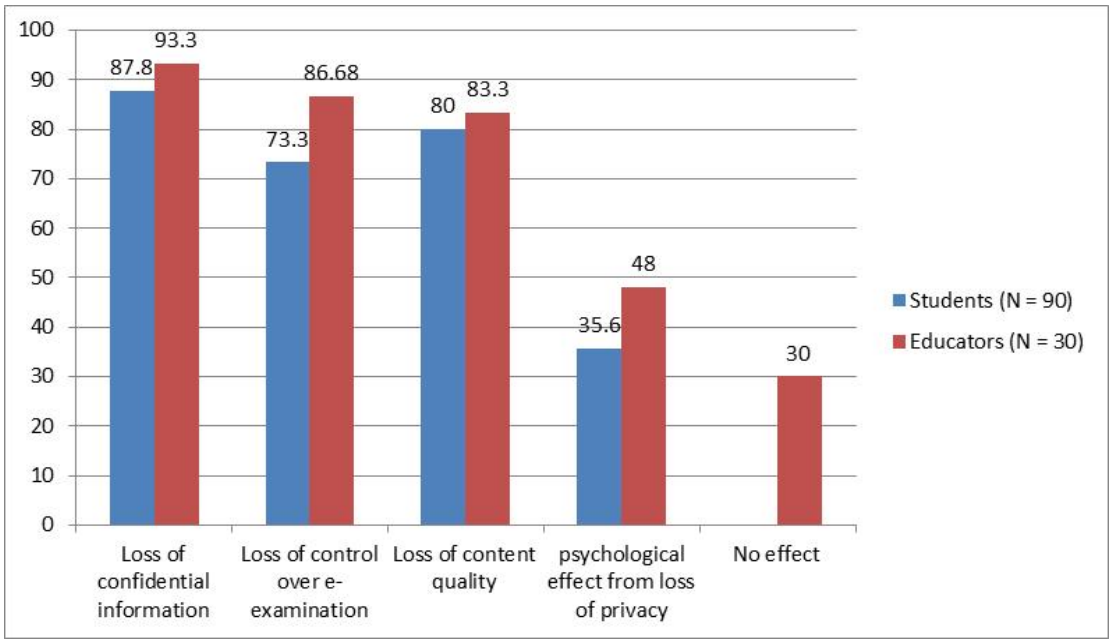

Fig. 2: Damaging effects of m-learning security threats to lecturers

5 DISCUSSIONS

The perceptions of the lecturers remain very important in the adoption, implementation and use of any mobile innovation in education system. While this study was focussed on educators' perspectives, learners' views were also obtained as they are stakeholders in mobile learning systems and their opinions on security issues that may affect their lecturers were also analysed.

The finding from research question 1, fig. 1 shows the security concerns instructors might face when using mobile devices as a teaching aid. The question was directed to the lecturers during the interviews and to the students in the questionnaire. 76.6% of the educators believed that privacy issues and exploitation of security breaches are concerns to them when using mobile devices for teaching and 84.4% of the students also agreed with this. This result is in line with the findings of the authors in [3], in which system and data security and actors' privacy are the first two challenges identified in m-learning. 53.3% of the educators indicated that interception of personal and confidential information by students and outsiders, either for fun or malicious acts, is a security threat for them, and 77.8% of the students also concurred. 60% of the educators were also concerned about virus and malware attacks on m-learning systems. This study supports the work of the authors in [9], which discusses the various forms of attacks as well as data interception that affect mobile device security.

Over 65% of the educators feared unauthorised access to learning content and unpermitted sharing of copyrighted e-materials by the students among themselves as security issues being perpetrated by learners in HEIs in Nigeria through mobile devices. This is made possible due to inadequate copyright laws and software piracy in Nigeria [10-11]. 46.6% of the educators believed that denial of service is a security risk to m-learning environment while 36.67% of them are of the view that propagation of false or misleading information using mobile devices among the learners is a threat to m-learning. This is quite common as some students spread incorrect information through social media [12]. However, 6.67% of the educators believed that m-learning poses no security threats to them when using mobile devices as a teaching aid or that any issues posed by the devices can be overcome successfully.

Fig. 2 (research question 2) shows the side effects of using mobile devices for teaching. 93.3% of the educators believed that loss of their confidential information is a major security consequence of m-learning. 87.8% of learners share the same view. The study is consistent with the work in [3] who state that loss of confidential information is one of the worries for lecturers in m-learning and their confidentiality should be guaranteed at all times. Similarly, educators would want their identities to

remain confidential to avoid falling victim to unsuspected criminals who can assume their identity to carry out malicious acts. 86.67% of the lecturers indicated that the loss of control mainly during e-assessment and e-examination is a threat to the lecturers. This can lead to examination malpractices and illegal collaboration during assessments if m-learning is not properly implemented. 73.3% of learners share similar views. This result is consistent with the study conducted by authors in [2], in which most of the educators believed that m-learning will ease examination malpractices. Again, the findings agree with that of the work in [3] which revealed that e-examination procedures carried out in an unsupervised or semi-supervised way is one of the difficult challenges within the m-learning context. Therefore educators, who are interesting in using any technology for educational purposes, will want to take ownership and control of such projects [2].

Over 80% of the educators believed that loss of content quality of learning materials is a likely side effect of introducing m-learning system that can make it possible for learners to tamper with learning materials if the security is weak. Altering learning content and grades without authorisation from lecturers and amending confidential documents can be feasible if there is a security breach in m-learning system known to the students. 80% of the learners supported this from the questionnaires. An m-learning system must be secured against manipulation and modification from legitimate users who are mainly students and unauthorised users. 48% of the educators interviewed agreed 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, 30% of the educators believed that m-learning poses no adverse effect to them in discharging their teaching delivery due to the fact that they adequate precaution when using their mobile devices and reluctantly use these as teaching aids [13-14]

It should be noted that responses of the participants and respondents most especially during the interviews were limited to their experience, their knowledge about m-learning and security issues surrounding m-learning environments as well as their mood at the time of the interview. Therefore, there may be some subjectivity in answers given to the interview questions. Similarly, some of the responses given by the students to the questionnaire may be subjective relying on theoretical knowledge rather than practical involvement with an m-learning system. However, the results of this study are consistent with other similar studies conducted earlier in the field as cited above.

6 RECOMMENDATIONS

Having discussed the issues pertaining to m-learning security as well as the damaging effects from educators' viewpoints, the challenge is to put in place strategies for alleviating these security issues relating to mobile learning system, starting from the mobile devices and including the servers and network infrastructure, by deploying proper security policies. Research question 3 of this study gives various recommendations for alleviating these security issues as discussed below.

The first solution for alleviating issues in relation to privacy and security breaches, as suggested by 83.3% of the educators, is having good security policies and measures in place in mobile learning systems. This includes provision of robust access control mechanisms for authentication and authorisation before permission is given to view or download learning content and materials. This further includes encryption of data on m-learning servers to safeguard learning content from-unauthorised copying and downloading, and protect examinations, assessment and feedback processes from attackers and impostors. Mobile devices should also be secured with device locks and encrypted if sensitive information is stored on them. However, data encryption should preferably be used in combination with other security measures and in case other protective measures failed, encryption will ensure that even if a hacker manages to gain access to sensitive data, the format will not be readable [15]. Modern biometric security measure like fingerprints, voice recognition, dynamic signature features and facial features can be very useful in m-learning for enabling post authentication and authorisation security. However, the use of biometrics specifically for the m-learning environment is still at an early stage [2]

In addition to these security measures, modern Digital Identity Management can be introduced to mobile devices to reinforce the security and privacy of m-learning systems. This involves assigning a unique digital identity to each learner after formal registration. Each mobile device will be registered as an attribute associated with its learner's digital identity. The mobile learning system will be responsible for managing the association between a user and their multiple handheld devices. Digital identity management can be used to enhance the level of privacy because only the mobile learning system

will know the relationship between the digital identity of a particular user and the identities of the mobile devices they use during m-learning activities [3].

Another suggested solution for alleviating the security issues given by 67% of the educators is the use of legacy protection mechanisms. This involves having regular data backup, installing firewalls on m-learning servers and having up to date anti-malware and anti-virus software installation on m-learning systems as well as installing all security patches. The result is supported by the work in [3] that discusses the security and privacy challenges of m-learning and suggests that educators should be extremely concerned about the safety of their data stored on mobile devices.

Having highly trained security experts during the design and development of m-learning systems and mobile apps is another recommendation given by the educators, and 63% of the respondents agreed with this. Security experts' opinions and contributions are very vital in ensuring threats free m-learning environments. However, many of the educators interviewed feared lack of security experts and staff competent with m-learning in Nigerian HEIs. The study is in line with work of the authors in [6] who state that lack of competent staff to support mobile teaching in Nigeria universities can derail mobile learning programs.

In tackling the sharing of copyrighted e-materials, a novel solution known as Digital Rights Management (DRM) can be used. DRM is a technology that can be used for content protection in m-learning environment. It is a class of access control measures that are used to limit the use of digital content and devices. A DRM based m-learning system can focus on learning content protection and other basic procedures of m-learning facilities that can be secured. Being an emerging technology, much research works on DRM is still ongoing [3]. All the recommended security measures can be validated by performing system review and assessment on the m-learning systems, analysing generated security logs, setting auditing features and alert, and evaluation of report by users of unusual behaviour of m-learning system and devices [16-17]

7 CONCLUSION AND FURTHER RESEARCH

While there are many issues that affect the acceptance of m-learning by some educators, such as hesitation in using new technology in their modules until they have evidence that it will benefit their teaching experience and enhance student learning [18] and lack of motivation or confidence to use ICT devices [19-20] the main discussion of this paper is the security and privacy aspect of m-learning. University scholars already have demanding careers in knowledge delivery and expanding research [21]. Their privacy and confidential information being exposed in the course of discharging their duties should not be a concern if adequate security measures are in place in m-learning systems. Similarly, loss of control during e-examinations and loss of content quality should neither be a concern nor source of worry for educators in a highly secured m-learning environment. A strong mechanism should also be put in place to prevent cheating through m-learning system [22]. These security barriers and the others identified above should be taken into consideration during the design and implementation of m-learning systems.

There is no doubt that patronage in mobile learning is going to increase as technology advances all, particularly in Nigeria which is ranked among the largest mobile market in Africa [23], therefore high levels of security must be maintained to avoid cyber-attacks on learning content and educators' privacy by having legacy protection mechanisms in place, robust access control in the form of modern digital identity management such as biometric features, as well as digital rights management. Furthermore, while educators are extremely concerned about the safety of their data stored on m-learning systems, engaging technical security experts during m-learning implementation and deployment so that specialised attention could be given to the development of secure gadget and apps will no doubt inspire lecturers' confidence in m-learning systems and mobile apps.

This paper has considered m-learning security from educators' perspectives, but future research work should focus on m-learning security based on other stakeholders in Higher Education Institutions, particularly the learners' because they are a major player in knowledge delivery [24]. Learners are more likely to have many security concerns in using their mobile devices for learning purposes since some of them are not security conscious like other stakeholders.

REFERENCES

[1] Sitthiworachart, J. and Joy, M.S. (2008). Is Mobile Learning a Substitute for Electronic Learning? In proceeding of: IADIS International Conference e-Learning 2008, Amsterdam. pp. 451 – 458

[2] 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*

[3] Kambourakis, G (2013). Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *International Journal of u- and e- Service, Science and Technology*. 6(3), pp.67-84

[4] Howell, M., Love, S. and Turner, M. (2008). User characteristics and performance with automated mobile phone systems. *International Journal of Mobile Communications*. 6(1), pp.1-15.

[5] Chidiogo, E (2013). Nigeria ranked sixth in Internet security threat. [Online] Available from http://telegraphng.com/2013/06/nigeria-ranked-sixth-in-internet-security-threat/ [Accessed on 10-January-2014]

[6] Umoru, T.A & Okeke, A.U (2012) M-Learning in Nigerian Universities: Challenges and Possibilities*. Global Awareness Society International 21st Annual Conference - New York City, May 2012*

[7] Adedoja, G., Botha, A., & Ogunleye, O. S. (2012). The future of mobile learning in the Nigerian education system. *IST-Africa 2012 Conference Proceedings, Dar es Salaam, Tanzania, 9-11 May 2012*

[8] Kagan, J (2014). The New Wireless Wave: Prices Falling, Cloud Rising. [Online] Available from http://www.ecommercetimes.com/story/79925.html#sthash.sMadKBnE.dpuf [Accessed on 10-March-2014]

[9] Obodoeze, F.C., Okoye, F.A., Mba, C.N., Asogwa, S.C. & Ozioko., F.E (2013). A Holistic Mobile Security Framework for Nigeria*. International Journal of Innovative Technology an Exploring Engineering (IJITEE).* 2 (3), pp.1-11

[10] Waziri, K. M. (2011). Intellectual Property Piracy and Counterfeiting in Nigeria: The Impending Economic and Social Conundrum. *Journal of Politics & Law* 4(2), pp.196-202

[11] Fabunmi, B. A. (2009). The Roles of Librarians in Copyright Protection in Nigeria. *International Journal of African & African-American Studies* 6(1), pp84-93

[12] Jegede, P. O. (2009). Age and ICT-related behaviours of higher education teachers in Nigeria. *Issues in Informing Science and Information Technology*, 6(2009), pp.770–777.

[13] 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*

[14] Lane, L (2014) Social media can aid spread of false information. [Online] Available from http://www.dailytoreador.com/opinion/article_c6496c06-87d4-11e3-b0c3-001a4bcf6878.html / [Accessed on 10-April-2014]

[15] Yong, J. (2011) Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes. *Journal of Universal Computer Science (J. UCS).* 17(2), pp. 296-310

[16] Stallings, W., & Brown, L. (2012) Computer Security Principles and Practice (2nd Edition) *Pearson Education Inc. Prentice Hall NJ*.

[17] Mitchell, C. J. (2004). *Security for mobility.* The Institution of Engineering and Technology, London. UK

[18] Kneil-Boxley, S. (2012). Towards a mobile learning strategy to support Higher Education. *Innovative Practice in Higher Education*. 1(2), ISSN: 2044-3315

[19] Agbatogun, A. O. (2013). Interactive digital technologies' use in Southwest Nigerian universities. *Educational Technology Research and Development*. 61(2), pp.333-357.

[20] Yusuf, M., & Balogun, M. R. (2011). Student-teachers competence and attitude towards information and communication technology: A case study in a Nigeria university. *Contemporary Educational Technology* 21(1), pp. 18–36

[21] Okebukola, P. (2006). Principles and policies guiding current reforms in Nigerian universities. *Journal of Higher Education in Africa* 4(1), pp.25–36

[22] Leung, A., Sheng, Y., & Cruickshank, H (2007). The security challenges for mobile ubiquitous services. *Information Security Technical Report*. 12(2007) pp.162 –171.

[23] Boyinbode, O. K., & Akinyede, R. O. (2008). Mobile learning: An application of mobile and wireless technologies in Nigerian learning system. *International Journal of computer science and network security*. 8(11), pp.386-392.

[24] Zamzuri, Z. F., Manaf, M., Yunus, Y.,& Ahmad, A. (2013). Student Perception on Security Requirement of e-Learning Services. *Procedia-Social and Behavioral Sciences*. 90(2013), pp.923-930.