Investigating Attack Vectors in M-learning Systems in Nigerian Universities

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 keen adoption of m-learning by higher education institutions on a global scale because of widespread use of mobile devices requires proper security considerations in order not to expose m-learning systems to cyber-attack. M-learning systems normally comprise three components which are the mobile device, one or multiple servers and network devices. While servers and network infrastructure have some inbuilt security and are usually owned by educational institutions or service providers, who have adequate resources to ensure their security, mobile devices are owned by individuals and generally do not come with protective software such as antivirus. Lack of security tools makes mobile devices vulnerable to many threats and attacks. The objectives of this paper are, therefore, to investigate which components of m-learning environments are prone to attack and what are the common attack routes in Nigerian universities. This paper will recommend solutions to these problems and the findings of this paper can help m-learning system developers to put more security measures on the components of m-learning system that are vulnerable to risks, threats and attacks.

Keywords: m-learning, security standards, attack, attack vector, threat, vulnerability point.

I. INTRODUCTION

Mobile learning focuses on mobility and learning through interaction with personal mobile devices. Although mobile devices were initially developed and primarily used as communication equipment like fixed wired telephone, researchers and telecommunication experts have been exploring ways of deploying mobile devices in learning and education [1]. The growing trend towards mobile learning can be explored to response to individual challenges in educational contexts, enhance formal learning, improve and assist learning for people across ages and augment learning opportunities, particularly in countries where educational opportunities are limited. However, along with mobile learning opportunities, there are some challenges that need to be addressed, one of which is lack of security in mobile technologies that may lead to attacks on personal and institutional data.

The security consideration of mobile learning is becoming increasingly important as more universities are deploying mobile technologies to complement their classroom learning delivery and the technology devices used in mobile learning can potentially become vulnerable if the security aspects are neglected. 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 [2]. Servers and network infrastructures can also be subjected to physical and digital attacks if not properly secured [3]. Threats or attacks can be app based, web based or through a network and an attacker only needs one vulnerable point of attack to succeed [4]; Therefore, m-learning systems must have comprehensive security measures in place by closing off all possible avenues of attack. The various attack routes in mobile learning environment in Nigerian Higher Educational Institutions (HEI) are discussed in this paper.

The first section of this paper is a review of related work on m-learning security attacks. It summarises existing work on mobile attacks and evaluates their various recommendations. The second part discusses the threats to the m-learning systems based on each component, that is, the mobile client, the servers, and the network infrastructure. The third part discusses the research carried out on security issues on various threats and attacks on m-learning system in Nigerian universities and details the purpose of the research, the methodology and research questions. A brief overview of the analysis of the results of the research is presented in section four of the paper while section five gives a detailed discussion on the results gathered. The last part of the paper highlights and discusses recommendations given to 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.

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

Digital cyber-attacks on mobile devices will continue to flourish because they are cheaper and less risky than physical attacks as hackers and cyber criminals only require a computer and an Internet connection to strike, in addition to the fact that the attackers are unrestrained by distance or geographical location and they are difficult to identify and prosecute due to the anonymous nature of the Internet [5]. A recent security report written by Nachenberg [6] reveals a rapid increase in the number of mobile device attacks which is expected to continue to rise significantly in the coming years [7]. Numerous threats are waiting to attack m-learners as the Internet proliferates with hackers and attackers. Tupakula and Varadharajan [8] state that mobile devices have limited resources to enforce strong security measures, making them easily vulnerable to attacks. The authors propose IPSec protocol traceback and prevention as techniques for counteracting denial of service (DoS) and distributed denial of service (DDoS) attacks on mobile nodes. Jang-Jaccard and Nepal [5] observe that cyber-attacks are increasing and becoming more attractive and potentially more destructive than ever before as mobile technologies are being embraced, and the numbers of victims of these modern attacks are also growing significantly. They argue that a malware is the key choice of weapon to carry out malicious intents using the emerging technologies such as social media, cloud computing and smartphone SMS. These two research projects focussed on DoS and DDoS attack on mobile devices and on malware classes – viruses and worms, Trojan horses and spyware. They shed little light on other attack methods and routes.

Tugui *et al.* [9] discuss the various components of an e-learning system that are susceptible to security attack and possible vulnerabilities that may affect the security of the online teaching and learning system such as DDoS, search-SPAM and keyloggers which may be installed by students to steal lecturers' passwords and modify grades without permission. Hasan et al. [10] agree that the security is an important aspect of open, interactive and distributed learning systems like e-learning or m-learning and that considerable effort should be put into development of the content and infrastructure for the online system to avoid attacks and ensure the reliability of technology to users. Levy *et al*. [11] conducted a study to assess the severity of security attacks on an e-learning system to determine the ethical implication of the attacks. The five types of security attacks investigated in their study are: attacks on the server, e-mail interception, unauthorized file sharing, unauthorized access and spoofing attacks. Their findings reveal that the 90% of the participants viewed the severity of these attacks as unethical while 3.24% of the participants reported these cyber-security attacks to be ethical. While these studies were based on security attack on an e-learning system, the results are applicable to m-learning systems to a large extent as m-learning is a subset and extension of e-learning [12 - 14].

Obodoeze *et al.* [15] identify five mobile security attack models in Nigeria. Their models include attack on mobile devices, internet/mobile network, corporate WLAN Intranet, telecom base station and physical attacks. The authors discuss frameworks based on the security triad of safety, attack and privacy that covers the physical, data and operational safety of mobile telecommunications infrastructure. They propose five security frameworks against attacks: on GSM data confidentiality and integrity, on a corporate network, against loss of mobile equipment or phone and bombing of mobile base stations, from malicious programs and hackers and malicious programs as a result of users' ignorance. Although all their proposed frameworks are suitable for preventing security attacks on mobile devices and infrastructure in general, they may not be easily adapted for mobile learning systems.

III. THREATS TO M- LEARNING SYTEMS

The variety of serious threats and various forms of attacks that affect m-learning systems are happening mainly due to vulnerabilities that remain in the m-learning development process. A typical m-learning system comprises server computer systems (application and database), web services, network infrastructure, and client mobile devices. Depending on the point of entry the threats that affect m-learning systems can be categorised into application-based, web-based, network-based and physical threats [16]. An application-based or mobile app threat is downloadable software that may pose security issues for mobile devices. Although a malicious mobile app may look genuine, it is purposely developed to attack, destroy, disable or commit fraudulent acts. Similarly, a good native app may have flaws in design or configuration which are then exploited, attacked or hacked for malicious reasons, and malware and spyware fall into this category of threats. A web-based threat is due to connectivity to the Internet and accessing deceptive or fraudulent websites using a mobile web app or mobile browser. Web-based threats include phishing, drive-by downloads and browser exploits. Most mobile devices normally support mobile networks as well as local wireless networks such as Wi-Fi and Bluetooth. These types of networks are vulnerable to network threats such as Wi-Fi sniffing and network exploits. Lost or stolen devices forma class of physical threat that is common to mobile devices. The mobile device is valuable not only that it can be stolen and re-sold, but more importantly that it may contain sensitive personal information. A survey on mobile device users showed that one out of every three mobile device users has lost their device at some point in time [17].

Other physical threats that affect servers and network infrastructure include physical damage to servers, routers,

switches, cabling plant or even base stations. These often happen during student riots in some universities in developing countries such as Nigeria, thus leading to unscheduled downtime or denial of service. Internet-connected servers in m-learning are also open to several threats and attacks that hackers are likely to use to either gain access or bring the servers down. These attacks include brute force attack, open relay, cross-site scripting, SQL Injection, and DoS/DDoS. Blended threats which involve a combination of attacks against different vulnerabilities may propagate into the m-learning systems. Having identified a number of threats to m-learning systems, research has been conducted to investigate the following questions in universities in Nigeria.

(1) *Which components of m-learning system are common to attack (mobile devices, servers or network devices)?*
(2) *How is the security of m-learning devices breached in Nigerian universities?*
(3) *What are the ways to reduce attacks on m-learning systems?*

IV. METHODOLOGY

In finding solutions to the research questions, data were collected on security issues being encountered by learners and lecturers in three universities in Nigeria. The study for which ethical approval at the authors' institutions had been granted, employed a survey research approach using a random sample population of students and academics in Computer Science departments. The data collection method involved delivering a set of questionnaires to 120 final year undergraduate students as well as interviewing a total of 30 lecturers in the same universities. The instrument for primary data was 21 questions divided into 4 sections. Demography for personal information was the section one while section two gathered data on various mobile devices owned by the participants and the type of activities they are used for. Section three collected data on mobile learning awareness and learning activities, and section four was based on security aspects of m-learning system. It obtained information about how the security of m-learning systems is breached. The section concluded with how to reduce attacks on m-learning system. Technical terms and concepts were explained briefly in the questionnaire and the researcher was available during the study to assist the respondents in understanding any part of the questionnaire.

A pilot study was conducted and recommendations given were taken into consideration in producing the final version of the instruments. A pre-test was carried out for the second time to ensure high reliability and understanding of the questions. The paper questionnaires were handed out after lectures while the link to the online version was given to the respondents if they which to complete it online at their discretion. Further interviews were held with academics in computer departments and were informed that their data will be stored fully anonymised. All the copies of the questionnaire that were administered were returned for analysis. The data obtained were analysed and presented using frequency distributions, pie charts, histograms and statistical tests.

V. RESULTS

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

A. *Research Question 1: Which component(s) of m-learning system is common to attack?*

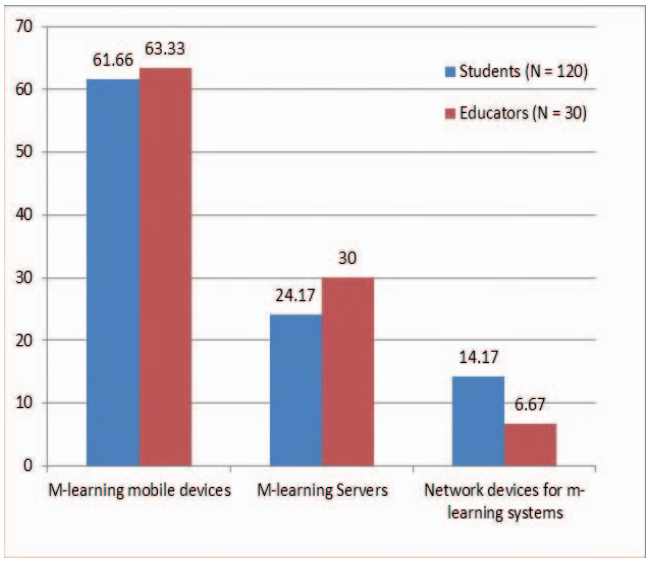

Fig. 1: What is the common attack point in m-learning system?

This section of the study shows that threats and attacks are more predominant on the mobile devices as perceived by the students and educators. Over six in ten, (63.33%) of the educators and 61.66% of the students responded that mobile devices are easily attacked. Server systems are next as indicated by one in ten (30%) of the educators and a quarter (24.17%) of the students. Network devices are believed to be least attacked as revealed by only 6.67% of the educators and 14.17% of the students respectively.
This result obtained was further analysed using the chi-square statistical test for dependency to compare the views of the students and educators on the most attacked components. The chi-square statistic is 1.3989, the P-Value is 0.496856 at the confidence interval of 0.050. The test shows that there is no significant difference between the students and academics on the component of m-learning

systems that is prone to attack. The test confirms that the opinions of the educators and students are the same on the severity attack on m-learning systems components.

B. *Research Question 2: How is the security of m-learning devices breached in Nigerian universities?*

This part is a follow up to research question one above. It aims to know how m-learning devices are breached and two questions were used from the questionnaire. The first is to determine if the security of the participants' device has been breached before. 81 out of the 120 students (67.5%) noted that the security of their mobile device has been breached or compromised before while 39 respondents representing 32.5% said their security of their device has never been breached.

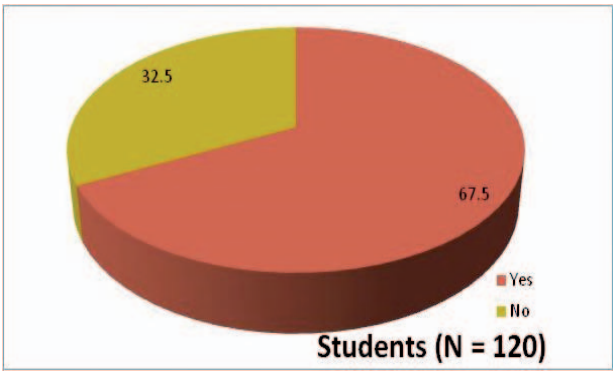

Fig. 2: Has the security of your mobile device been breached before?

The second question is to investigate how the security was breached. Fig. 3 below indicates one or more ways the security of the respondents' devices were breached. We observed that 65.43% of the students indicated that they have no password lock on their mobile devices. Bluetooth sharing was left by around seven in ten (69.14%) of the students leading to security attacks. Attacks through mobile browser accounted for 64.2% on how m-learning systems were breached. Malicious attachments to SMS or emails and downloads from unknown sources or websites have significant percentages on how security of mobile devices are breached or compromised as shown in fig. 3. The educators' views were also obtained through interview to determine how m-learning devices can be breached. More than half of the educators (53.55%) indicated no password lock on mobile devices can lead to security breach. Two thirds of the educators (66.67%) responded that 'Bluetooth left on' after sharing is a security risk. Based on educators' opinions, attacks through mobile browser accounted for 56.67% of the perceived security breach while malicious attachments to SMS or emails and downloads from unknown sources or websites have 63.33% and 46.67% respectively.

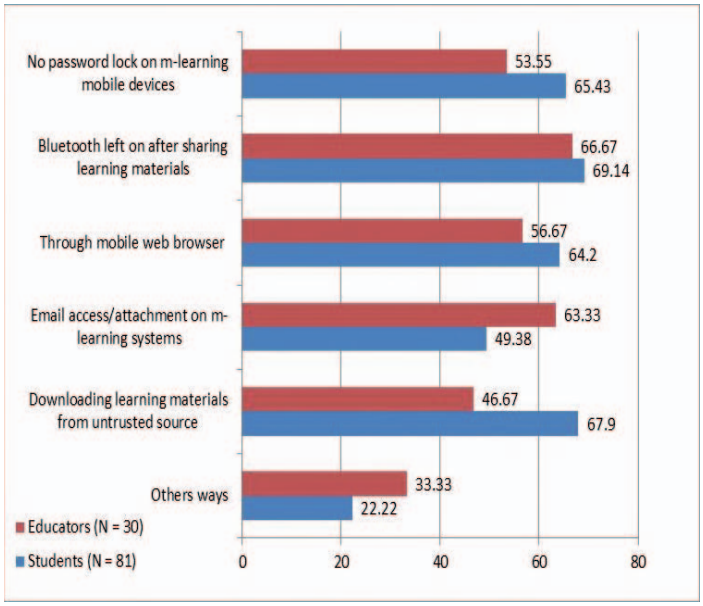

Fig. 3: How is the security of m-learning devices breached?

A statistical test for observable differences linked to the students and educators on how the security of their mobile devices was breached was carried out using nonparametric Mann-Whitney U Test. Table 1 and 2 below show the statistical calculations. According to the table 2, there is significant difference on the security breach experienced by the students and educators. This implies that the students and educators security breaches experience different security breaches.

Table 1: Ranking of students and educators on security breach

Dimension	# of Participants	mean of ranks	sum of ranks
Students	81	9.17	55
Educators	30	3.83	23
Total	111	6.5	78

Table 2: Mann- Whitney test

Test	Security breach
U Mann - Whitney	2
Z	2.482
Asump. Sig (2-tailed)	0.01314

VI. DISCUSSION

Fig. 1 shows that mobile devices have higher numbers of security threats and attacks than servers and network devices combined. This higher numbers may be due to a couple of reasons. According to Stamford [18] an estimated two billion smartphones and other mobile devices will be shipped before the end of 2014 for general use including formal or informal education. Similarly according to Guo *et al.* [19] the total number of smartphones and tablets shipments has passed the number of the PCs and notebooks. As more mobile devices are produced, more of them are likely to come under attack from operating system vulnerabilities [20]. This suggests that the number of attacks on mobile devices is likely to increase with the number of such devices being used by students for learning purposes.

Furthermore, servers and network devices are normally manufactured to specific security standards including factory fitted security software such as firewall and defenders, mobile devices generally do not come with security software. M-learning servers and network devices owned by educational institutions or service providers, who have adequate resources to ensure their security and even mandate manufacturers to customise inbuilt security on the servers before delivery, mobile devices owned by individual students are rolled out to the public and are difficult to customise for each and every student. An exception to this is mobile devices acquired by HEIs for use by their students.

Fig. 2 shows that higher numbers of the participants have had their mobile devices breached before while fig. 3 reveals how the devices are breached based on students' experience and educators' perception. The highest percentage of the breaches (69.14%) was committed when the Bluetooth of the device was left on. Many users do not know that they have to disconnect or switch off their Bluetooth connectivity when they are through with the usage, thereby giving access to unknown connections through which malicious programs can be passed to user's device later on. Tipton and Nozaki [21] indicate that several design flaws exist in the Bluetooth protocol as well as its implementation which mobile malware exploit to spread. According to Clooke [22], the first known mobile malware, Cabir, spread through Bluetooth. Although malware spreads through mobile devices communicating using Bluetooth, typically within a few meters range, the spread can be rapid across many devices if there are many collections of Bluetooth-enabled devices. Such an attack was reported during World Athletics Championship in 2005 where many people who attended the event had their devices infected with malware within a short time [23].

Visiting unfamiliar websites and downloading learning materials from unknown sources most especially among students can lead to serious security breach as they accounted for 67.9%. Mobile viruses spread the same way a traditional computer virus does through download of an infected file to the mobile device over the internet [22]. This practice includes file-sharing downloads, mobile apps downloads from un-trusted sites and false update patches. In addition, when infected webpages are browsed by using a mobile device browser, the malicious code hidden in the webpage may be triggered. This malicious code may infect the mobile device and cause some damage [24] and it is more common among learners than educators. While the educators and students shared experienced similar security breaches, a large difference is noticed on downloading learning materials from unknown sources. This may be due to the fact that students download learning materials more than lecturers and some of them may download from illegitimate and untrusted source. This implies that while the educators are engaged in uploading learning materials to m-learning systems, students are normally busy downloading materials from both legitimate and illegitimate sources, thereby exposing themselves to cyber-attacks.

Malware, spyware and other malicious attacks are also spreading through SMS (Short Message Service), MMS (Multi Media Service), IM (Instant Messaging) and other messaging services by attaching themselves to the message as shown in figure 3. This finding is supported by Faiz and Maqsood [25] who reveal that ComWar is the second landmark mobile malware that spreads by sending itself via MMS to all contacts in the address book. Furthermore, Shih *et al.* [24] observes that as mobile IM usage grows, new forms of attacks on mobile devices are likely to appear, such as hijacking lists of IM names and sending links to recipients directing them to malicious sites. Mobile viruses can also send fake IM messages with the malicious code attached. Many users do not bother to password protect their devices making them vulnerable to unauthorised use which accounts for 65.43% of security breaches among students. Categorised under other ways of attacks in the study are malware that infect mobile devices by exploiting vulnerabilities in Wi-Fi connectivity. Worms that spread by exploiting vulnerabilities in Wi-Fi connectivity could also infect mobile devices that are Wi-Fi capable [26]. Similarly, vulnerabilities exist in the operating systems used by mobile devices. There are reported cases of vulnerabilities in the design of some mobile operating systems that have caused the mobile device to work very slow or even crash [23].

While the participants were informed to answer the questionnaires from experience they have had on m-learning system, some students might have answered the questionnaires partly on their theoretical knowledge rather than security issues they experienced individually when using their mobile devices supposes. Therefore, there may be subjectivity in the answers given by the participants. Nevertheless, the results obtained from this study are accurate and consistent with related studies conducted in the field of m-learning in other parts of the world.

VII. RECOMMENDATIONS

Having highlighted the components of m-learning systems and identified that mobile device is the predominantly attacked component and discussed how the security of m-learning systems are breached, the challenge is to ensure that learning systems are secured, right from the mobile devices, to the servers and network infrastructure. Since servers and network devices used for m-learning are usually owned and managed by Higher Educational Institutions or service providers, they have enough resources to engage the service of security experts to protect these two components by deploying proper security policies.

C. Research Question 3: What the ways to reduce attacks on m-learning systems?

Based on the data presented above and the literature review, the following are recommendations to reduce the security attacks that are specific to m-learning mobile device clients which is perceived to have the highest number of security breaches among the three components of m-learning system.

- All mobile devices have security settings, their security features should be turn on. Automatic updates should also be turned on as these updates often contain changes that make the mobile device more secure.
- Since mobile devices do not come with antimalware by default, anti-virus, anti-malware and firewall apps if available should be installed on their operating systems as soon as they are acquired.
- Security apps such as phone finders and remote wipe should be installed in case of lost or theft to prevent unauthorised access to confidential and private information as well as learning materials stored on the devices.
- Each Bluetooth interface should be highly secured and put on non-discoverable mode if available. It should be turned off immediately after use and connection from an unknown source should not be accepted in any case.
- Users should avoid connecting to unsecured free public Wi-Fi when connecting to m-learning servers while on the move as the connection may be intercepted by hackers.
- Unsolicited emails should never be responded to, neither their attachment opened using m-learning devices. Adverts and pop-ups should be discarded or blocked.
- Private or personal information and learning materials should not be stored on the devices as much as possible and if they must be stored, they should be properly encrypted.
- It is safe to have password lock or biometric access in order to prevent unauthorised use or access to learning content. Password lock should be enforced on m-learning devices and changed regularly.
- Apps and learning materials should be downloaded only from trusted sources, such as the official m-learning system and installation of applications from unusual or suspicious sources should be avoided.
- Data on the m-learning device should be backed up regularly either to a memory card (which should be kept in a safe place) or kept on a cloud storage. Alternatively, the device can be set up to synchronise data each time it is connected to a computer.
- M-learning users should not open multimedia messages (MMS) or attachments in emails, or click on links in emails and SMS messages unless they expecting them and they are sure that the messages are from trusted sources.
- Unusual behaviours on m-learning devices could be a sign that they are infected. These behaviours may include unusual text messages and actions such as interface change which was not done by the user.

VIII. CONCLUSION AND FURTHER RESEARCH

The security aspect of m-learning is often ignored when mobile devices are used for educational purposes. However, m-learning devices are prone to security threats or attacks and the user's confidentiality, integrity and data availability are at stake [27]. The purpose of this paper is to spot the predominantly attacked components of m-learning, understand how the security is breached and reduce the occurrence of the attacks. Following a research study, mobile device component of an m-learning system was identified as the easiest attacked component while file sharing through Bluetooth and downloading of learning materials and content from unreliable sources are the main attack routes in Nigerian universities.

A failure in any component of m-learning environment will lead to failure for the entire system, a highly secure mobile learning environment is supposed to detect and deter threats and attack as well as having no known vulnerability weak points and unsusceptible to failure. This paper has discussed security attacks surrounding mobile client of m-learning systems in Nigerian universities and gave recommendations on preventing the threats. Future work can focus on other components of m-learning system including servers and network infrastructure and the collective responsibilities of m-learning stakeholders in combating security attacks.

Extensive work has been done on many areas of m-learning security such as m-learning security issues from lecturers'

perspectives [28]. Future research work can be done on collective responsibilities of m-learning stakeholders in overcoming the security issues and broad comparison review on e-learning security and m-learning security.

REFERENCES

[1] J. Sitthiworachart and M. S. Joy "Is mobile earning a substitute for electronic learning?" In proceeding of: IADIS International Conference e-Learning 2008, Amsterdam, pp. 451 – 458, July, 2008

[2] M. Howell, S. Love and M. Turner "User characteristics and performance with automated mobile phone systems." International Journal of Mobile Communications, vol, no.6, pp. 1-15, January, 2008

[3] T. Dimkov, W. Pieters and P.Hartel "Portunes: representing attack scenarios spanning through the physical, digital and social domain". In Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security Springer Berlin Heidelberg, 2011, pp.112-129, 2011

[4] A. Leung, Y. Sheng, and H. Cruickshank "The security challenges for mobile ubiquitous services". Information Security Technical Report, vol. 12, no.3, pp.162 – 171, May, 2007

[5] J. Jang-Jaccard and S.Nepal "A survey of emerging threats in cyber security". Journal of Computer and System Sciences, vol. 80, pp. 973–993, February, 2014

[6] C. Nachenberg " A window into mobile device security". Symantec Security Response (2011): pp. 4-9, 2011, Available online from http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf Accessed on [April 20, 2012]

[7] E. Geier "2012 in Security: Rising Danger", Available online from http://www.pcworld.com/article/242174/2012_in_security_rising_danger.html, Oct. 20, 2011. [Accessed on March 10, 2012]

[8] U. Tupakula, U and V. Varadharajan "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, 2013, vol. 21, pp. 374 – 381, September, 2013

[9] O. Tugui, S. Funar, and A. Cofari "Trends of integrating the e-learning platform in the graduate agronomic educational system in Romania". Bulletin of University of Agricultural Sciences and Veterinary Medicine Cluj-Napoca. Horticulture, vol. 65, no.2, pp.621-626, 2008

[10] S. H. Hasan, D. M. Alghazzawi, and A. Zafar "E-Learning systems and their Security" BRIS Journal of Adv. S & T (ISSN. 0971-9563) vol.2, no 3, pp. 83-92, 2014

[11] Y. Levy, M. M. Ramim and A. R. Hackney "Assessing ethical severity of e-learning systems security attacks" Journal of Computer Information Systems, vol. 53, no.3, pp.75-84, Spring,2013

[12] T.H. Brown "Towards a model for m-learning in Africa", International Journal on E- learning, ISSN 1537-2456, vol. 4, no.3, pp. 299-315, 2005

[13] H. H. Yang "New world, new learning: trends and issues of e-learning" Procedia - Social and Behavioral Sciences, vol.77, pp.429 – 442, April, 2013

[14] L. T. Brown "The role of M-learning in the future of e-learning in Africa" A paper presented at 21st ICDE World Conference, 2003, Available online from http://www.naun.org/journals/educationinformation/eit-12.pdf. [Accessed on July 26, 2010]

[15] 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

[16] Lookout "Mobile Threats, Made to measure" 2013, Available online from https://www.lookout.com/resources/reports/mobile-threat-report [Accessed June 10, 2013]

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

[18] C. Stamford "Gartner says worldwide traditional PC, tablet, ultramobile and mobile phone shipments on pace to grow 7.6 percent in 2014". 2014, Available online from http://www.gartner.com/newsroom/id/2645115 [Accessed on May 20, 2014]

[19] M. Guo, P. Bhattacharya, M. Yang, K. Qian and L. Yang "Learning mobile security with android security labware" In Proceeding of the 44th ACM technical symposium on Computer science education, ACM, pp. 675-680, March, 2013

[20] M. La Poll, F. Martinelli, F and D. Sgandurra "A survey on security for mobile devices" Communications Surveys and Tutorials, IEEE, vol. 15, no.1, pp. 446-471, First Quarter, 2013

[21] H. F. Tipton and K. M. Nozaki "Information Security Management Handbook" (6th edition). CRC Press, Taylor and Francis Group. Florida, 2012

[22] R. Clooke "Mobile security- History of mobile malware" 2013, Available online from http://www.mobilesecurity.com/articles/421-history-of-mobile-malware-part-i [Accessed on June 26, 2013]

[23] A. Gostev "Mobile malware evolution: an overview, part 1", 2006, Available Online from http://www.viruslist.com/en/analysis?pubid=200119916 [Accessed on August 02, 2012].

[24] D.H Shih, B. Lin, H. S Chiang and M. H Shih "Security aspects of mobile phone virus: a critical survey." Industrial Management and Data Systems, ISSN: 0263-5577 vol.108, no.4, pp. 478- 494, 2008

[25] A. Faiz and M. Masqood "Information security threats against mobile phone services (Developer's Perspective)" 2009, Available online from https://pure.ltu.se/portal/files/31139724/LTU-PB-EX-09046-SE.pdf [Accessed June 22, 2014]

[26] C. R. Mulliner "Security of smart phones (Doctoral dissertation, University Of California Santa Barbara)", 2009, Available online from http://www.lib.unb.ca/Texts/PST/2005/pdf/debbabi.pdf [Accessed June 20, 2013]

[27] T. S. Yap, T.S. and H. T. Ewe "A mobile phone malicious software detection model with behavior checker" Web and Communication Technologies and Internet-Related Social Issues-HSI 2005, Springer Berlin Heidelberg, vol. 359, pp.57- 65, 2005

[28] 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 in Barcelona, Spain, 7 – 9 July 2014.