Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.8, No.1, 2018

E-Learning Security Challenges, Implementation and Improvement in Developing Countries: A Review

Abdulrahman Saidu[1] Mohammed Abubakar Clarkson[2] Mohammed Mohammed[3]
1.Department of Computer Science, Federal Polytechnic Bali Taraba State, Nigeria.
2.Department of Agricultural Technology, Federal Polytechnic Bali Taraba State, Nigeria
3.Department of Computer Science, Federal College of Education Yola, Adamawa State

Abstract
The application of e-learning technology in teaching and learning environment in developing countries has created a significant impact especially to students and staff. Despite the fact that it attended a high level of acceptability, there are various security threats and implementation challenges militating against effective utilization of the e-learning platform. This paper, reviewed the impact associated with security vulnerabilities and implementation issues that impede successful e-learning implementation. Specifically, the review examined the effect of security challenges in e-learning and viability of e-learning implementation. This review found that there is need to develop a viable and holistic approach model that combines both biometric fingerprint and cryptography authentication techniques for the e-learning platform. It is recommended that there is need for adequate and uninterruptable bandwidth and power supply for e-learning sustainability.
Keywords: security challenges, implementation, e-learning, ICT and trustworthiness.

Introduction

The application of E-learning technology in knowledge delivery is receiving great attention because it facilitate teaching and learning activity. According to Almarabeh, (2014), e-learning refers to the "use of Information and Communication Technology e.g. internet, computers, Mobile phone, Learning Management System (LMS), Televisions, Radios and others to enhance teaching and learning activities". Similarly, e-learning has been defined as the use of electronic media, Information and Communication Technologies (ICT) in education (Saidu, 2014). The new technologies including ICT and e-learning have become the driving forces in most tertiary institutions today (Tarus, 2015). It has been adopted globally and to a greater extent in the developed and a few in the developing countries. However, with its application worldwide, e-learning has not been utilized optimally in education in Nigeria (Atsumbe et al 2012). This is likely due to some challenges that tend to militate against the use of this facility in the universities, polytechnics and colleges of education across the country. The aim of this paper is to review and fetch together a series of current literatures in the area of e-learning environment. The paper is reviewed based on a number of subheadings that comprises the effect of security challenges in E-learning, the viability of e-learning implementation, conclusion and recommendations.

The Effect of Security Challenges in E-learning

Recent researches show that there are security challenges in e-learning platform environment which need to be enhanced. Miguel et al (2014a) argued that security requirements cannot be accomplished with technology alone; hence new models such as trustworthiness approaches could complete the technological solutions and support the e-assessment requirement for e-learning. The paper proposed a methodological approach to build a normalized trustworthiness model. In line with this, Miguel et al (2014b) claimed that security vulnerabilities in on-line assessment impede the development of an overall model devoted to manage secure on-line assessment. They authors presents an innovative prediction approach for trustworthiness behavior to enhance security in online assessment and this indicated that neural networks may support e-assessment prediction. Nevertheless, Miguel et al (2014a) and Miguel et al (2014b) suggested future work that will improve security issues in e-learning. The published paper by Miguel et al (2014c) justifies the need of trustworthiness model as a functional requirement devoted to improve information security. The study further revealed that there are relevant drawbacks that obstruct e-learning designers to provide adequate reach security requirement defined by e-learning stakeholders.

In a study by Miguel et al (2013d) found that high drop-out rates, poor grading, plagiarism and security vulnerabilities, such as anomalous authentication are the major impediment of e-learning. This is supported by Shonola, and Joy (2014) that the use of mobile technology for learning poses a threat to confidentiality, integrity and privacy of the data involved in learning delivery for both learners and lecturers. The research further revealed that (i) virus/malware attack (ii) student exploiting security breach/privacy issues (iii) data interception for malicious acts (iv) unauthorized access to learning content and (v) unpermitted sharing of copyright e-learning materials, are issues militating against e-learning activities. In a research conducted by Miguel et al (2014e) shown that in spite of the recent information security enhancement developed, it failed to integrate holistic security models as required. Based on these needs the paper proposes an innovative approach for modelling trustworthiness in the context of secure learning assessment online collaborative learning groups. The paper suggested that future

research looks at benchmark for each Learning Management System (LMS) to be used in pilot, considering performance factors in real paralleling platforms. This is in agreement with Shonola, and Joy (2014) that certain learning Management System (LMS) which support multiple authentication methods are likely to be applied simultaneously buy users methods.

From the above review, Miguel et al (2014a) proposed a methodological approach for building a normalized trustworthiness model as solution to security challenge for e-learning. However, this approach is not viable to predict trustworthiness students' behavior and evaluation alert for anomalous result as outlined by the authors. Similarly, Miguel et al (2014b) presented an innovative prediction approach for trustworthiness behavior to enhance security in online assessment but the major drawback of this approach is that, the neural networks need to be implemented by combining the training methods. Likewise, Miguel et al (2014c) justified the need of trustworthiness model as a functional requirement devoted to improve information security and proposed an innovative trustworthiness and security methodological approach to develop secure Computer Support Collaboration Learning (CSCL) activities. However, further deployments which is likely to require large amount of data analysis, the research recommends further work that will investigate parallel processing methods to manage trustworthiness factors and indicators. Equally, Miguel et al (2013d) provide a good model of flexible authentication system that will meet each and every type of course and user profile but certain LMS that support multiple authentication methods are likely to be applied simultaneously buy users methods. In the same way, Miguel et al (2014e) propose modelling trustworthiness for secure online learning assessment with collaborative learning groups. Yet the study showed that there is need for hybrid assessment model which could combine technology security solutions and functional trustworthiness measures. They authors suggested future research that looks at benchmark for each LMS to be used in pilot, considering performance factors in real paralleling platforms. Shonola, and Joy (2014) reported some security threats that are posed to the confidentiality of data integrity in e-learning delivery for both learners and lecturers and made a vital solution to them. However, the authors recommended that future work is highly needed on M-learning security based on stakeholders in higher educational institutions.

The Viability of E-learning Implementation

A research carried out by Almarabeh (2014), examined students' perception of E-learning at the University of Jordan based on Technology Acceptance Model (TAM). Sampling and measurement analysis were used to carry out the study. The research reveals that the students are highly qualified and accepting the E-learning system with the desire to use it in more advanced manner. This result is sustained by (Adewole-Odeshi, 2014), which looked at the relationship between attitude and e-learning with application of Technology Acceptance Model (TAM) and the findings displayed that students have positive attitude towards e-learning acceptability. Similar methods were adopted for implementing the studies.

A study conducted by Nguyen et al (2014) explored the relevant concepts of E-learning, cloud computing, and to indicate the cloud-based E-learning benefits in respect of consumer innovativeness. The methodology adopted was structured survey with a set of all scales referring to the different variables identified in the model. The findings indicated that the adoption of cloud-based E-learning is influenced by performance expectancy, social influence, hedonic motivation, and habit. The research concluded by proposing a model of E-learning adoption that will explain the factors of influence on the consumer intention and the use of cloud-based E-learning system and interestingly the model was empirically tested and basically supported.

In a study by Adebayo & Abdulhamid (2014) examined the impacts associated with challenges and security lapses of the existing electronic-examination system with aim of upgrading and developing a new e-examination system that takes care of the challenges and security gaps associated with the existing systems. The methodology accepted for the study was interviews and questionnaires. The result exposed that the new system uses data encryption in order to protect the questions sent to e-Examination center through the internet or intranet and a biometric fingerprint authentication to verify the stakeholders.

Kamba (2009) examined and discussed the problems, challenges and benefits of implementing E-learning in Nigerian universities. Survey methodology was adopted for the study. The result found that awareness of e-learning among the universities is very high but investment and commitment to develop an e-learning application is very poor and below expectation. This assertion conforms to Almarabeh (2014) and Adewole-Odeshi (2014). Moreover, the research outlined that lack of sufficient trained ICT professional has been a recurring focus in ICT. Also, the study further revealed some factors affecting successful implementation of e-learning in Nigerian Universities such as: (i) Inadequate instructional materials (e-books, CD-ROM), (ii) Lack of tutorial support from instructors, coaches, tutors or technical staff (iii) Poor telecommunication tools like internet facilities, (iv) Lack of collaboration for social communication learning with the instructional demand for active learning, (v) Irregular supply of electricity, (vi) Insufficient fund to upgrade and maintain the equipment and facilities, (vii) Bad policy implementation, and (viii) Lukewarm attitudes towards e-learning process by staff and students. These claims were maintained by (Sife, et al 2007) who further argued in agreement with Tarus et al. (2015) that ICT implementation

challenges include (i) lack of awareness and attitudes towards ICTs (ii) inadequate technical support (iii) transforming higher education (iii) lack of staff development and ownership .In depth review of related work was adopted for the review of the paper. Furthermore, the result obtained by (Kamba, 2009) shown that most common encountered problems are unreliable internet connection and mobile lines, slow access to website due to insufficient bandwidth and limited number of computers connected to the internet.

Georgiev (2006) in a study on transition from e-learning to m-learning examined the challenges in the transition from e-learning to m-learning. The paper revealed that, (i) technological challenges for the developers result from the features of the mobile devices such as: less powerful, less memory, less computing power, smaller screen size, and lack of keyboard (in most cases). Another challenge is that, the developers must know all the abilities and shortfalls of a particular mobile device and communication technologies to successfully design and develop a mobile learning system. Likewise, educators need to know how to operate mobile device to a degree where they are convinced of their potential for educational users. Similarly, educators must also know what to require from the developers and to know what limits of such systems are**.** Students have to know the abilities and limitations of their personal mobile devices when presenting educational content. (ii) Development challenges; defining what type of mobile system to be developed with the consideration of information transfer speeds at different wireless technology. Another developer's challenge is the issue of the loss of connection and choice of development platform as well as the ability to test mobile learning system. Educational content development is the main challenge of educators. (iii) Pedagogical challenges; most of the developers are computer science professional and have little knowledge about different pedagogical approaches. Knowing technological limitations of the mobile devices is another developers challenges. Educators need to find useful way to combine the new communication and mobile technologies with different pedagogical approaches. A pedagogical challenge to students they need to be self-organized in order to achieve the required goal.

Tarus et al (2015) in a study on challenges of implementing e-learning investigated the challenges hindering the implementation of e-learning in Kenya public universities. The study employed a hybrid methods of descriptive research design. In addition to those mentioned earlier, the research also identified challenges that are impediments to e-learning implementation to include: (i) inadequate ICT and e-learning infrastructure, (ii) lack of affordable and adequate internet bandwidth, (iii) lack of technical skills on e-learning and e-content development by the teaching staff, (vi) lack of interest commitment among the teaching staff to use e-learning and (v) insufficient time required to develop e-learning content. Furthermore, the investigation by Qureshi et al (2012) aimed to identify issues that are related to e-learning in Pakistani university through the feed-back captured from students and provide strategist to successfully overcome the issues. The methodology adopted for the study is in-depth literature review and discussions with the students. The findings demonstrated electricity failure and English proficiency as the most significant barriers to successful integration of e-learning. Also, the study revealed that technical assistance and private issues are still confronting e-learning implementation.

It could be understood from the review above there some weaknesses of the viability of E-learning implementation. Almarabeh (2014) suggested that TAM model should be examined with teachers from university of Jordan to get more comprehensive view of E-learning system perception. However, the major drawback of the study is that it failed to give a full test of TAM, where the actual technology used was not included in the research model, therefore, the actual technology needed to be added to examine the whole TAM model. Nguyen et al (2014) concluded by proposing a model of E-learning adoption that will explain the factors of influence on the consumer intention and use of cloud-based E-learning system and the model was empirically tested and basically supported. This is a good proposal but the model has limitation and the paper proposed future work that could combine the effect of the elements, expand the research scope, object, adjust scales, and add more variables to the research model. Similarly the result of Adebayo & Abdulhamid (2014), conveyed that the new system will use data encryption in order to protect the questions sent to e-Examination center through the internet or intranet and a biometric fingerprint authentication to verify the stakeholders. However, the study concludes that the new system is not fully implemented, but will reduce the problems associated with the e-examination when implemented. Also (Adewole-Odeshi, 2014), revealed that no attempt was made to study attitude of students towards e-learning based on anxiety towards computer, security and suggested future work that will determine if a significant relationship exists between attitude towards e-learning and other variables (anxiety towards computer and security). In the same manner, Kamba (2009) addressed factors affecting successful implementation of e-learning in Nigerian universities and also found the most common encountered problems to the e-learning implementation but the result of the research did not substantially cover security challenges of e-learning implementation**.** In the same vein Sife et al (2007) discovered that there are various ICT challenges that impede the implementation of e-learning and yet the solution proffered is not viable to handle the existing problems. The study further argued that, universities in developing countries should adopt e-learning technologies to improve teaching and learning process.

Tarus et al (2015) concluded that successful implementation of the recommendations made by the study can easily be achieved if the impediments of E-learning are squarely addressed. Although, the recommendations are quite relevant but not substantial because security weakness of the e-learning has not been taken care of which is

very essential. Equally, Qureshi et al (2012) uphold that electricity failure, English proficiency, technical assistance and private issues are confronting e-learning implementation and further recommended (i) using open source software and receiving funding from government and public private partnerships, (ii) blended learning techniques involving a balanced mix of face to interactions, self-space learning and online interactions and (iii) sitting up national e-learning centers for e-learning activities within the educational institutions. This assertions are significant, nevertheless, the issue of security vulnerability was not properly addressed.

A research paper by Georgiev (2006) examined the technological, development and pedagogical challenges in transition from e-learning to m-learning that really affects developers, educators and students. The paper concluded that, successful solutions to the current and future challenges could be eliminated only if the cross-interactions between educators, developers and students in the m-learning process are taken into account. This is noteworthy conclusion which could be integrated not only as an authors' opinion but a generalized concept.

Conclusion

E-learning security and implementation challenges have been extensively reviewed and from the literature it was found that there are various challenges militating against successful implementation of e-learning platforms. Although, various vital solutions were proposed for the challenges confronting e-learning environment and they were not viable enough. Therefore, there is need to develop viable and holistic model approach that will bridge the gap of security vulnerabilities and implementation impediments in e-learning atmosphere.

Recommendations

From the range of literature reviewed above the following recommendation were drawn:

- The government could provide adequate funding that will take care of e-learning platform implementation
- Regular training of stake holders (especially staff and students) on the use of e-learning environment.
- Developing a workable and holistic e-learning platform model approach that will make use of both biometric finger print authentication and cryptography for protecting the integrity of data
- Government could provide good policy and laws that will regulate security bridges in e-leaning atmosphere.
- Adoption Collaboration and partnership with international Databases providers such as IEEE, Google Scholar, and Elsevier could be encourage.
- Use of blending learning techniques involving a balanced of mix of face to face interactions, self-paced learning and online interaction (Qureshi et al 2012).
- Government could provide adequate and uninterruptable internet bandwidth and power supply or could involve private participation in the provision of these infrastructure.

Reference

Adebayo, O., & Abdulhamid, S. M. (2014). E-Exams System for Nigerian Universities with Emphasis on Security and Result Integrity. *arXiv preprint arXiv:1402.0921*.

Adewole-Odeshi, E. (2014). Attitude of Students Towards E-learning in South-West Nigerian Universities: An Application of Technology Acceptance Model. *Library Philosophy and Practice*, 0_1.

Almarabeh, T. (2014). Students' Perceptions of E-learning at the University of Jordan. *iJET*, *9*(3), 31-35.

Georgiev, T., Georgieva, E., & Trajkovski, G. (2006, June). Transitioning from e-Learning to m-Learning: Present issues and future challenges. In *null* (pp. 349-353). IEEE.

Kamba, M. (2009). Problems, challenges and benefits of implementing e-learning in Nigerian universities: An empirical study. *International Journal of Emerging Technologies in Learning (iJET)*, *4*(1).

Nguyen, T. D., Nguyen, T. M., Pham, Q. T., & Misra, S. (2014). Acceptance and use of e-learning based on cloud computing: the role of consumer innovativeness. In *Computational Science and Its Applications–ICCSA 2014*(pp. 159-174). Springer International Publishing.

Miguel, J., Caballé, S., Xhafa, F., & Prieto, J. (2014, May). Security in Online Learning Assessment Towards an Effective Trustworthiness Approach to Support E-Learning Teams. In *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on* (pp. 123-130). IEEE.

Miguel, J., Caballe, S., Xhafa, F., Prieto, J., & Barolli, L. (2014, July). Towards a normalized trustworthiness approach to enhance security in on-line assessment. In *Complex, Intelligent and Software Intensive Systems (CISIS), 2014 Eighth International Conference on* (pp. 147-154). IEEE.

Miguel, J., Caballé, S., Xhafa, F., Prieto, J., & Barolli, L. (2014, September). Predicting trustworthiness behavior to enhance security in on-line assessment. In *Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on* (pp. 342-349). IEEE.

Miguel, J., Caballé, S., & Prieto, J. (2013, September). Providing Information Security to MOOC: Towards effective student authentication. In *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on* (pp. 289-292). IEEE.

Qureshi, I. A., Ilyas, K., Yasmin, R., & Whitty, M. (2012). Challenges of implementing e-learning in a Pakistani university. *Knowledge Management & E-Learning: An International Journal (KM&EL)*, *4*(3), 310-324.

Shonola, S. A., & Joy, M. S. (2014, July). Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)'. In *6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain. pp. 7081* (Vol. 88).

(Saidu, 2014). Management Information System for E-learning: A Case Study of Federal Polytechnic Bali. *In Computer Engineering and Intelligence System,* 2014 ISSN 2222-2863 (online) on (pp. 29-38), Vol.5 No.4

Sife, A., Lwoga, E., & Sanga, C. (2007). New technologies for teaching and learning: Challenges for higher learning institutions in developing countries.*International Journal of Education and Development using ICT*, *3*(2).

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). Challenges of implementing e-learning in Kenya: A case of Kenyan public universities. *The International Review of Research in Open and Distributed Learning*, *16*(1).