Security Challenges in Accessing E-Learning Systems

Ekereke, L. & Akpojaro, Jackson
[1]Department of Mathematical Sciences
Faculty of Basic and Applied Sciences
University of Africa
Toru-Orua, Bayelsa State, Nigeria
E-mails: ekerekelayefa@rocketmail.com, jackson.akpojaro@uat.edu.ng
Phone: +2348138803299

ABSTRACT

Advancements in Information and Communication Technology (ICT) has put e-learning platforms as effective systems for training and learning, cost effectiveness, accessibility and flexibility of time and place. Different e-learning systems have been effectively deployed by many tertiary institutions in Nigeria, particularly for distance learning programmes. ICT has transformed the focus of teaching and learning from the traditional or distance education to electronic-based with high value-added and resourceful education. However, security of e-learning systems has been one of the key research issues in the literature. The Internet as the backbone of the e-learning systems is inherently insecure. Information security and privacy concerns in e-learning environment are very crucial because of the multiple users who are communicating via the Internet. As a result of this interconnectivity, data or information are exposed to several security threats and vulnerabilities. This study presents a thorough review of security issues and concerns of e-learning systems. Thereafter, we present the studies that address various issues of e-learning in the context of Nigeria environment. The security challenges encountered by e-learning platform in tertiary institutions in Nigeria and measures for addressing them are presented. The paper is concluded by recommending some salient remedies to ensure secured e-learning environment in Nigeria.

Keywords: E-learning systems, Internet, environment, Data, Information & Tertiary institutions.

iSTEAMS Proceedings Reference Format
Ekereke, L. & Akpojaro, Jackson (2019): Security Challenges in Accessing E-Learning Systems.
Proceedings of the 15th iSTEAMS Research Nexus Conference, Chrisland University, Abeokuta, Nigeria, 16th – 18th April, 2019. Pp 11-20
www.isteams.net - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V15N1P2

1. INTRODUCTION

The advancements in information communication technology (ICT) has pushed e-learning to the fore front of tertiary education in Nigeria due to the ease in training and learning, easy accessibility, cost effectiveness, and flexibility of the venues and time of lectures (Bhuasiri et al, 2012). ICT has indeed transformed the pattern of education and training from the traditional or distance education to electronic-based highly flexible and resourceful education. E-learning in this context is referred to as an educational system that is based on information and communication technology system. E-Learning is constructed in a variety of contexts, such as distance learning, online learning, and networked learning and learning to promote educational interactions between students, lecturers and learning communities (Karforma et al, 2009). It can also be referred as a situation where learning is accomplished over internet-based delivery of contents and programmes.

As the web remains an ideal platform for offering a lot of related information to the learners, it has been adopted as a mean for the interaction with learners and other information systems (IS) such as e-learning. Moore et al (2012) pointed that E-learning environment is an IS based on World Wide Web (WWW) and it consists of learning management system (LMS), knowledge management system (KMS), content management system (CMS) or content authoring tools. The Internet is one of the primary means of implementing e-learning and the Internet faces a number of illegal activities and security threats. E-learning is a multiuser environment having shared information and most probably accessed through Internet which makes it security sensitive. Hence, the issue of security threat, attacks, vulnerability and risks cannot be avoided in the e-learning environment (Chen and He, 2013).

Moreover, most of the e-learning environments (e.g., LMS, KMS, etc.) have one level of information security mechanism or the other in place up to an extent such as authentication, authorization, granting access only on the basis of user unique login and password (Assefa and Solms, 2009). However, only this security measure (login and password) is not safe enough for its users. Therefore, we present the study that addresses some salient issues of e-learning in the context of Nigeria environment. Section 2 gives a brief literature review, section 3 explores e-learning system in Nigeria, and section 4 exposes the existing security issues and concerns of e-learning systems. Thereafter, we present various studies that addressed the security challenges encountered by e-learning platforms in tertiary institutions in Nigeria and measures for addressing them in section 5. The paper is concluded in section 6 by recommending some salient remedies to ensure secured e-learning environment in Nigeria.

2. RELATED WORKS

Wu et al (2012) gave a good remark of e-learning. E-learning was described as an innovative approach to education. It is seen as a digital medium for passing knowledge from instructors to their students as well as a medium that eases information dissemination among learners. It is a modern way of education delivery via electronic media to boost learners' knowledge and enhance their learning capability or skills. Education delivery through e-learning methods could be classified into synchronous and asynchronous learning. Synchronous learning occurs real-time, in which the instructor and learners are present virtually at the time of learning content delivery. Students log in at a prearranged time and communicate with the instructor and peers. In asynchronous learning, the lecturer and students are not present at the time of content delivery (Negash et al., 2008).

Another area covered in e-learning is the change brought by the advent of Web 2.0 technologies, which focus on people interactions and collaboration within a community (Greenhow et al., 2009). Web 2.0 applications such as blogs, wikis, social media or social networking sites allow a learner to interact with other learners, gain from one another experience and develop their own knowledge. Thus, Web 2.0 has the potential to provide students with learning experiences that are meaningful, collaborative, and socially relevant. The emergence of Web 2.0 came along with e-learning 2.0.

While Web 2.0 technologies use social media for socializing and connecting friends, family and collaboration within a social community, e-learning 2.0 caters for the educational aspect, and is an improvement on the formal e-learning platform. Apart from receiving, reading, and responding to learning content in a conventional e-learning environment, e-learning 2.0 also permit learners to create content and to collaborate with group peers to form a learning network with delivery of content creation.

Also, a number of security issues in e-learning systems have been investigated in previous studies. (Levy, 2011) discussed user authentication as an important issue to consider in e-learning security. The work shows that with varying software and hardware requirements, policies and strategies should be put in place to ensure appropriate authentication of the learner.

May and George (2011) focused on privacy and security issues in e-learning and came up with some issues such as digital right management, protection of personal data, address and location privacy, authentication, anonymous use, etc. The work stated that learners are concerned with the protection of their sensitive data while technology providers are finding ways of securing the learning environment and also the storage of learners' data.

Barik and Karforma (2012) also discussed various security risks (or threats) in e-learning. Some of which include confidentiality violation, integrity violation, denial of service, etc. and providing remedies to minimize all these risk. Chen and He (2013) highlighted identity theft, impersonation, and inadequate authentication as some security issues in online learning systems. Saleh and Wahid (2015) also mentioned confidentiality, integrity, availability, authenticity, and access control as various sources of e-learning security threats. Adetoba et al (2016) opined that interoperability of applications, standardization and compatibility, security policies, and lack of e-learning infrastructure can be a security challenge.

3. E-LEARNING IN NIGERIA

E-learning is defined by various authors according to their personal knowledge and perspectives, but they all seem to agree that e-learning in the broadest sense can be seen as learning that occurs on line through the Internet, off the using of CD-ROM or other facilities such as radio, television and telephony (Ravichandra, 2005). Generally, e-learning is seen as electronic method of learning which is associated with internet-based learning. E-learning education in summary is the integration of modern telecommunication facilities and ICT resources, precisely the Internet, into the education system. In Nigeria, the use of telecommunication began in 1886 when a cable connection was established between Lagos and the colonial office in London. In 2001, Global System for Mobile (GSM) was introduced in Nigeria and this promoted the use of electronic means of communication and later triggered the introduction of e-learning through ICT.

As telecommunication services are increasingly improving, conventional universities in Nigeria are carrying out their academic activities through one form of ICT or the other. Due to the ever growing demand for tertiary education, the first e-learning tertiary institution, the National Open University of Nigeria (NOUN), was established in July, 1983 by an Act of the National Assembly to augment the traditional means of face-to-face classroom instructional delivery. Various studies regarding adoption, promotion and implementation of e-learning systems have been conducted in Nigeria. However, these identified studies have confirmed some diverse issues like technological, infrastructural, user satisfaction, internet availability, bandwidth etc. as illustrated in Table I.

Table 1. Identified studies addressing various e-learning issues in the context of Nigeria environment.

Identified Issues/Challenges	Citation
Inability of teachers to assist the students develop the ability and knowledge necessary to make them use the e-learning effectively.	Olutola et al (2015)
High primary cost of infrastructural development and to increase public access to internet and other ICTs.	Bibiana, et al (2015)
Internet Connectivity, Inequality of access to the technology itself by all the students, School Curriculum, Attitude of Students, Software and License cost, and Electricity.	Stephan (2012)
Non-inclusion of ICT programs in teacher's training curricula and at the basic levels of education (such as Basic schools and secondary schools).	Timothy et al (2008)
Limited expertise for Maintenance and Technical Support	Oye et al (2011)
Lack of required skills, lack of access to ICT, and the location of the learner are critical factors that pose barriers to learning for students from lower socio-economic background like most students in Nigeria.	Clarke (2002)
Lack of qualified teachers to teach ICT in schools, increased moral degradation and burglary	Torruam, (2012)

Despite all the challenges/issues faced by e-learning in Nigeria tertiary institutions, there are currently at least nine ICT for education initiatives at various stages of development being carried out by the education coordinating agencies of government and ministry of education in Nigeria. These include:

- The Nigerian Universities Network (NUNet) project
- The Polytechnics Network (PloyNet) project
- The School Net project
- The Nigerian Education, Academic, and Resaerch Network (NEARNet)
  The Teachers Network (TeachNet) project
- National Open University
- National Virtual (Digital) Library (Ministry of Education/NUC)
- National Virtual Library (Ministry of Science and Technology/NITDA)
- National Information, Communication and Education Programme of the Presidency.

Though, most of the institutions of higher learning in Nigeria have started building their ICT centers but their main focus is to put up an internet facility without including much e-learning components.

4. E-LEARNING SECURITY ISSUES

E-learning offers students' considerable benefits including increase access to learning opportunities, convenience of time, and place, making available a greater variety of learning resources, improve opportunities for individualized learning and emergence of more powerful cognitive tools. However, the students and as well the teachers are venerable to a lot of insecurity while accessing e-learning systems. Security is a serious issue as ICT is used to transform and transfer knowledge in the educational sector. Primarily, there are four main stakeholders of the e-learning system. These include;

a) Developers: they design the instructions, also called Learning Objects (LOs), and upload on the servers in the form of web utilities. Learning Objects are the entities in electronic form. They may be a text, an audio, a video, a power point presentation for online courses.
b) Instructors: these are the tutors.
c) Administrator: Administrator maintains the material on server and controls the services. Learner access the LOs through network (Internet).
d) Learners: these are the students.

The relationship between these stakeholders is shown in Figure 1.

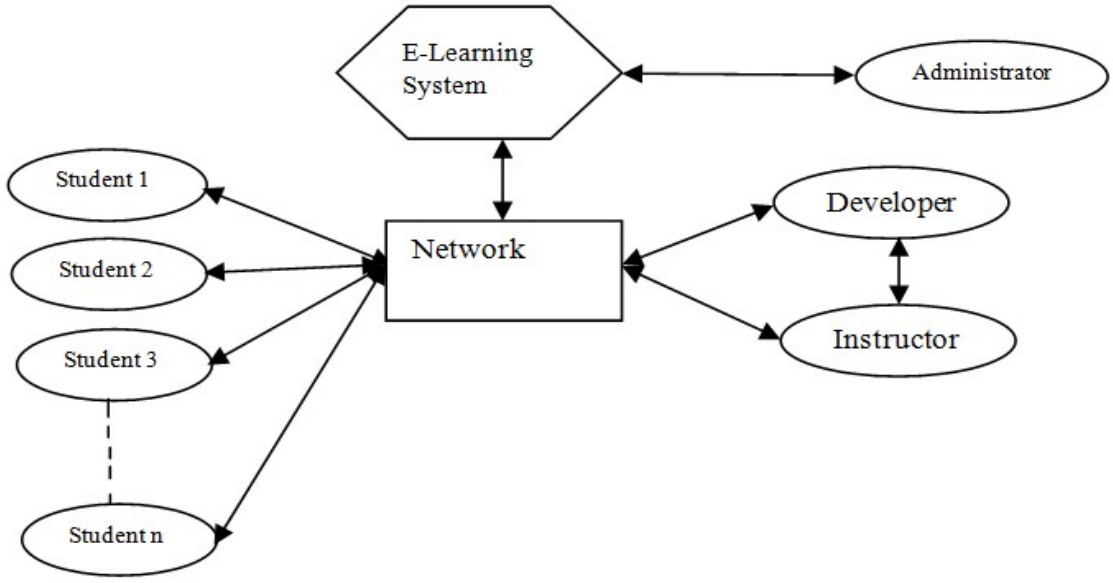

Figure 1: E-learning access model

From Figure 1, e-learning systems have multiple users and hence work in distributed environment connecting web and network resources together. Therefore, it is more sensitive to security issues. Security and privacy is one of the crucial concerns in e-learning educational context where enrolment of learners in online courses progressively increases (Luminita, 2011).

The major security issues come from both the network and the web security like availability, confidentiality, integrity and so on. Other e-learning security issues include;

- **Confidentiality violation:** Confidentiality is the protection of the assets of e-system from unauthorized access or user and modification. Confidentiality violation is a situation that occurs when an unauthorized party gains access to the assets present in E-Learning system. Numerous security risks can arise in e-learning that disrupt privacy and confidentiality of users. The learners need assurance that the data and information in e-system remain secure and private and never expose to unauthorized entities, devices or systems (Kim, 2013; Raitman, Ngo, Augar, et al, 2005).
- **Integrity Violation:** In network security, integrity means that data has not been altered. Data integrity defines the accessibility, reliability, correctness and high quality of stored data (Durairaj and Manimaran, 2015). Integrity is the assurance that only authorized users or programs has right to modify data or executable programs. Integrity Violation is the process whereby an unauthorized party gains access and temper with an asset used in E-Learning system. Integrity depends on access control.
- **Authenticity of information:** It is necessary to confirm the source of any and every information received for secure communication. Each user has unique identity that should be protected and checked before access and transmission of data. Rapid development in Internet technology makes it easy for the criminal to hack the users' identity. Hence, reliable identification of the learner is one of the essential factors of e-learning environment as it is the basis for access control. Once the user is identified then it is required to verify that the learner is the same as the person is claiming to be (Assefa and Solms, 2009). Each identity in e-learning environment is unique due to specific characteristics and preferences. These characteristics may include password, login information, courses taken etc.
- **Denial of Service:** Prevention of legitimate access rights by disrupting traffic during the transaction among the users of E-Learning system.
- **Authorization:** This is the feature that enables legal users to access the information as per their defined privileges. E-learning system lies under distributed system and multiple users are accessing it from different and several locations. Therefore, there is need of securing authentication mechanism not only to recognize the user but also determines the users' access privileges on the e-learning system so as to avoid Illegitimate use or Exploitation of privileges by legitimate users.
- **Malicious program:** Lines of code to damage the other programs.
- **Availability:** Availability of the system is referred to as the extent to which the system is available for learners whenever it is required (Behkamal, Kahani, and Akbari, 2009). It is vital to note that information and communication resources are always available when demand is raised so that the authorize learners may submit their assignments, comments, notes or papers within the specified time. If the user is not able to access the required material on time they may be frustrated or lose their interest.
- **Traffic analysis:** Leakage of information by abusing communication channel.
- **Masquerade:** A way of behaving that hides the truth by hackers.

5. SECURITY MEASURES FOR E-LEARNING

Accessing E-Learning system face different risks or threats as discussed in the previous section. In other to minimize this menace, the Following techniques may be adopted by e-learning systems to buff its security;

Digital Watermarking: This technique allows an individual to add hidden copyright notices, audio, video, image signals. So multimedia database server of e-Learning system may be protected against unauthorized use by the way of digital watermarking. Also e-Learning information like question papers, important study materials, etc is invisible to the viewer so the chances of hacking will be nil or less.

Access Control Using Firewall: A firewall is a combination of hardware and software security system established to prevent unauthorized access to a corporate network from outside the organization. It is a combination of packet filters and application (or circuit) gateways that can block some incoming traffic but permit e-Learning users (may be Students, Instructor, etc.) inside to communicate freely from the outside. The main principle based on the rule is that all traffic from inside to outside and vice versa must pass through the firewall. To achieve this, all access to the local network must first be physically blocked, and access only via the firewall should be permitted. Only the traffic authorized as per the local security policy should be allowed to pass through. It is the sole duty of all system administrators to earn knowledge and skills to implement firewall, to configure the firewall and to monitor & troubleshoot firewalls.

SMS Authentication: In Nigeria, the use of mobile phone is increasing day by day. Presently, over one third of the population of Nigeria use cellular phone as compared to the computer users. With such growth of telecom and mobile industry these mobile phones can be used for authentication purposes. It would be proper to use SMS for secure access of e-learning system. Possible procedure may be divided into two steps. In first step, a student submits the user ID and password through his/her cellular phone. In response to this e-learning system generates a special code and sends it to the registered phone of the user by SMS, which is actually the key for the current session. In the second step, student enters this code in order to authenticate his identity and access the e-learning system safely. This simply can be done by adding a cryptographic algorithm that takes username and password as input and provide output in the form of random/unique pass code. This code is sent to user's registered mobile phone not only to identify but also to authenticate and authorize the all kinds of users with pre-granted privileges.

Dual or triple authentication Method: Two-step authentication method is more secure than the single authentication method. First it is required to login using ID and passwords and after that it is required to authenticate sending an email or by short message using hand held device or biometrics or smart card or digital signature or digital certificate or a combination of three of the mentioned methods. This type of re-authentication has successfully been implemented by various secure web application systems like e-banking.

Cryptography: Confidentiality of a system ensures that information and data are not disclosed to any unauthorized person. Also readers must able to rely on the correctness of the content. One of the techniques in this aspect is cryptography. Different cryptographic tools and techniques are needed for the implementation of security in internet based transactions. There are two types of algorithms in cryptography namely; Secret-key algorithms: In secret-key algorithms the encryption and decryption key is the same, it requires the sender and receiver to agree on the key prior to the communication, the main function of this algorithm is encryption of data. Examples of such algorithms are Data Encryption Standard (DES), International Data Encryption Algorithms (IDEA), and Advanced Encryption Standard (AES). So only for encryption techniques for E-Learning content we can use these techniques.

Public-key algorithms: Public key cryptosystems, on the other hand, use one key (the public key) to encrypt messages or data, and a second key (the secret key) to decrypt those messages or data. Here three mathematical models are mainly used - Integer factorization, discrete logarithms and elliptic curve. We can use these techniques at the time of sending question paper and receiving answer sheets. To authenticate a participant we can use either the public key algorithm or digital signature.

Biometrics Authentication: Using password is an old and widely used mechanism and has good results in many cases incurring minimum cost. Still there is a chance of stealing or forging the password. Attacker can forcefully get the sensitive data like passwords through pre-functioned software (Aïmeur, Hage. and Onana, 2008). But Biometrics authentication method has proved its way through all this means of access control is specific and private to its user so it is very unique and the safest of all.

6. CONCLUSION

Some major security issues encountered by e-learning system of education have been explored in this study. User's privacy and his personal identity is the most crucial issue in a shared e-learning system. Beside authentication and authorization, non-availability of the system or e-contents to the learner at the required time frame is one of the major threats to the e-learning system. If the system is not available, it is totally useless for the learners and also may cause the frustration from the e-learner. Moreover, various methods of authentication have been discussed and are not found to be secure and reliable. Authentication of the learner is quiet difficult as anyone can get access on behalf of the registered user. Hence, in order to cope with such authentication concerns, e-learning systems are required to deploy security services such as access control, encryption, authentication, biometrics, and if possible combining them in the best capacity to getting the best way out to managing users and their privileges. Few security remedies have been suggested in this study. It is recommended that existing e-learning environments adopted by tertiary institutions in Nigeria should embed the security measures described in above to mitigate the security risk, though no system is absolutely secured. Moreover, the data transfer between the system and administrators or content operators or learners should employ a combination of encryption techniques. A secure learning platform should not only incorporate all the aspects of security but also make most of the processes transparent and easier to the teachers and the students so that it can be attractive to all.

REFERENCES

1. Adetoba, B. T., Awodele, O. & Kuyoro, S. O. (2016). E-learning security issues and challenges: A review. Journal of Scientific Research and Studies, 3(5): 96-100.
2. Aïmeur, E., Hage. H., & Onana, F. S. M. (2008). Anonymous credentials for privacy preserving e-learning in e-technologies. International MCETECH Conference, IEEE.
3. Assefa. S., & Solms. V. (2009). An information security reference framework for e-learning management systems. (ISRF e-LMS). Proceedings of 9th IFIP WCCE 2009.
4. Barik, N, & Karforma, S. (2012). Risks and remedies in e-learning system. International Journal of Network. Security. Application, 4(1): 51-59.
5. Behkamal. B., Kahani. M., & Akbari. M. K. (2009). Customizing ISO 9126 quality model for evaluation of B2B applications. Information and software technology, 51(3): 599-609.
6. Bibiana, N. N., Titus, A. U., & Jonathan O. O. (2015). The challenges of e-learning in tertiary institutions in Nigeria. International Conference, The Future for Education, 2nd edition.
7. Bhuasiri, W., Xaymoungkhoun, O., Zo, H., Rho, J. J., & Ciganek A. P. (2012). Success factors for e-learning in developing countries: A comparative analysis between ICT experts and faculty. Computers & Education, 58(2): 843-855.
8. Chen. Y. & He, W. (2013). Security risks and protection in online learning: A survey. The International Review of Research in Open and Distributed Learning, 14(5).
9. Clarke, A. (2002). Online Learning and Social Exclusion. NIACE, Leicester.
10. Durairaj. M., & Manimaran. A. (2015). A study on security issues in cloud based e-learning. Indian Journal of Science and Technology, 8(8): 757-765.
11. Greenhow, C., Robelia, B. & Hughes, J. E. (2009). Learning, teaching, and scholarship in a digital age Web2.0 and classroom research: what path should we take now? Educational Researcher. 38(4): 246-259.
12. Karforma, S., & Basudeb, G. (2009). On Security issues in e-learning system. Proceedings of COCOSY-09. University Institute of Technology, Burdwan University.
13. Kim. H. (2013). E-learning privacy and security requirements: Review. Journal of Security Engineering, 10(5): 591-600.
14. Levy, D. (2011). Lessons learned from participating in a connectivity massive online open course (MOOC). In Y. Eshet-Alkalai, A. Caspi, S. Eden, N. Geri & Y. Yair (eds.); proceedings of the Chais conference on instructional technologies research: Learning in the technological era, 31-36. Available online at http://www.openu.ac.il/research_center/chais2011/download/f-levyd94_eng.pd
15. Luminita. D. C. C. (2011). Security issues in e-learning platforms. World Journal on Educational Technology, 3(3): 153-167.
16. May, M., & George, S. (2011). Privacy concerns in e-Learning: Is using a tracking system a threat? Intentional Journal of Information Education Technology, 1(1):1-8.
17. Moore, J. L., Deane C. D., & Galyen, K. (2012). E-Learning, online learning, and distance learning environments: Are they the same? The Internet and Higher Education, 14(2):129-135.
18. Negash, S., Whitman, M, E., Woszczynski, A, B., Hoganson, K., & Mattord, H. (2008). Handbook of Distance Learning For Real Time and Asynchronous Information Technology Education. Hersey, IGI Global: Information Science Reference
19. Olutola, A. T., & Olatoye, O. O. (2015). Challenges of E-Learning Technologies in Nigerian University Education. Journal of Educational and Social Research, 5(1): 301-306.
20. Oye, N. D., Salle, M., Iahad, N. A. (2011).Challenges of E-Learning in Nigerian University Education Based on the Experience of Developed Countries. International Journal of Managing Information Technology (IJMIT), 3(2): 39-48.

21. Raitman. R., Ngo. L., Augar. N., & Zhou. W. (2005). Security in the online e-learning environment. Advanced Learning Technologies, ICALT Fifth IEEE International Conference on IEEE.
22. Ravichandran, V. (2005). E-learning or virtual learning through VSAT, A paper presented at the F19 working week in Egypt, pp. 5.
23. Saleh, M. M., & Wahid, F. A. (2015). A Review of Security Threats by the unauthorized in the E-learning. International Journal of Computer Technology, 14(11):6240-6243.
24. Timothy. O. A., Ibrahim, O. S., & Femi. A. A. (2008). E-Learning and distance education in Nigeria. The Turkish Online Journal of Educational Technology (TOJET), 7(4), Article 7.
25. Torruam. J. T. (2012). Application of e-teaching and e-learning in Nigerian educational system. Academic Research International, 3(1).
26. Wu, W. H., Wu, Y. C. J., Chen, C. Y., Kao, H. Y., Lin, H. & Huang, S. H. (2012). Review of Trend from Mobile Learning Studies: A meta-analysis. Computers and Education 59: 817-827.