ISSN No:-2456-2165

# Security Challenges in Accessing E-Learning Systems: A Case-Study of Sagbama, Bayelsa State

[1]Ekereke, Layefa, and [1]Akpojaro, Jackson
[1]Department of Mathematical Sciences
Faculty of Basic and Applied Science University of Africa
Toru-Orua, Bayelsa State
Nigeria

**Abstract:- Information and Communication Technology (ICT) advancement has put E-learning platforms as effective systems for training and learning. The platform is cost effective, easy to access and lecture time/place is flexible. Different E-learning systems have been effectively deployed by many tertiary institutions in Nigeria, particularly for distance learning programs. 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, the secureness of the E-learning systems has been a key research issues in the literature. The backbone of the e-learning system is the Internet and as such, it is inherently unsecure. Information security and privacy are very crucial because of the multiple users who are communicating via the Internet. As a result of information sharing over the internet, data are open to several security threats and vulnerabilities. This study presents a thorough review of security issues encountered by using E-learning platform for Educational delivery in Nigeria, we also review some related literatures. 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.*

## I. INTRODUCTION

Recent development in information communication technology (ICT), ease of access and lecture time and place flexibility has pushed E-learning to the fore front in the delivery of education(training and learning) across the world (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 captured in a variety of context, such as distance, online, or networked learning and it promote educational interactions between students, lecturers and learning communities (Karforma et al, 2009). It can also be referred as a situation where education is accomplished over internet-based delivery. As the web remains an ideal platform for passing a lot of related information to the learners, it has been adopted as the basic means for the interaction with learners and other information systems (IS). Moore et al (2012) pointed that E-learning platform is an IS based on World Wide Web (WWW) which consists of learning management systems (LMS), knowledge management systems (KMS), content management systems (CMS).

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 E-learning security issues in context of the Nigeria environment. The rest of this work is arranged as follows: Section 2; gives a review of some available literature, section 3; explores E-learning system in Nigeria, and section 4; exposes the existing security issues and concerns of E-learning systems. Thereafter, various studies that addressed the security challenges encountered by E-learning platforms in tertiary institutions of Nigeria and measures to addressing them are given in section 5. The paper is concluded in section 6 by recommending some salient remedies to ensure secured E-learning environment in Nigeria.

ISSN No:-2456-2165

## II. RELATED WORK

Wu, W., et al (2012) gave a good remark that E-learning is an innovative approach to education. It is seen as a computerized medium for passing knowledge from instructors to students and also a medium that eases information sharing among learners. It is seen as modern ways of delivery education via electronic medium to improve learners' know how and enhance their learning capability. Education delivery through e-learning methods could be classified into synchronous learning and asynchronous learning. The first occurs real-time, in which the instructor and learners are both present virtually at the time of learning or content delivery. Students log in at a prearranged time and communicate with the instructor and peers. In the later, neither lecturer nor students is present at the moment 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 an area (Greenhow et al., 2009). Web 2.0 are applications like blogs, wikis, social media or social networking sites allow a learner to discuss with each other, benefits from one another experience and develop their own basic knowledge. Thus, Web 2.0 has the potential to provide students with already trained learning experiences that are meaningful, collaborative, and socially beneficial. The emergence of Web 2.0 came along with E- learning 2.0. While Web 2.0 technologies uses social media for socializing and connecting friends, family and collaboration within a social community, E-learning 2.0 caters for educational need, and is an improvement on the formal E-learning platform. Apart from receiving or reading or responding to learning content in a conventional E-learning environment, e-learning 2.0 also permit learners to also create content and to collaborate with groups to form a learning network.

Also, a number of security issues have been investigated by previous researchers in their studies. Levy, 2011 missioned that user authentication as a vital issue to consider in E-learning security. His research shows that with the presence of different software and hardware requirements, policies must be put in place to make sure the learners are appropriately authenticated. May., et al 2011 in their research looked on insecurity and Privacy in E-learning and fore saw some issues such as digital right management, protection of personal data, address and location privacy, authentication, anonymous use, etc. their research stated that learners are looking forward to a system that can protect their sensitive documents while system providers are looking for ways of improving the system security of the learning environment and also a more secured way to store learners' documents.

Barik and Karforma 2012 also looked at different security risks (threats) in E-learning. Some threats disclosed include; violation of one's integrity, confidentiality violation, service denial, etc. and provided remedies to mitigate the risks. Chen and He, 2013 highlighted stealing of identity, impersonating, and half authentication as some major security issues facing the online learning system. Saleh and Wahid, 2015 also mentioned lack of confidence, lack of integrity, network unavailability, authenticity and lack of proper access control measures as few among various 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.

## III. E-LEARNING IN NIGERIA

E-learning has been defined by various authors according to their individual knowledge and perspectives, but they all seem converge at a point that e-learning in the broadest sense can be seen as educational delivery via on-line with the presence of Internet, away from the use mechanical facilities e.g. CD-ROM, radio, television e.t.c. Ravichandra, 2005. Generally, E-learning is seen as a digital pattern of education that is associated with using internet based facilities. In summary, E-learning is the integration of recent Telecommunication facilities and resources that has to do with ICT, precisely Internet, into the pattern of delivery of education. In Nigeria, use of telecommunication generally started in 1886. Then a cable was connected between Lagos and our colonial office in London. In 2001, Global System for Mobile (GSM) was introduced to Nigeria and this promoted using of electronic means of communication in the country and later triggered the introduction of e-learning through ICT.

As telecommunication services are increasingly improving, conventional universities in Nigeria are using one type of ICT or another to carry out their academic activities. Due to recent growth in the search for tertiary education, the first E-learning tertiary school, the NOUN (National Open University of Nigeria) was born. This was established in the year 1983, July an Act of the Nigerian National Assembly.

As a result of this, different studies regarding adoption, promotion and implementation of E-learning systems for educational purpose has 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 below;

ISSN No:-2456-2165

| Identified Issues/Challenges | Citation |
|---|---|
| Some of the teachers lack the technical know-how due to lack of constant usage to mentor students in developing their ability and knowledge necessary to make them use the e-learning effectively from the scarce. | Olutola et al (2015) |
| Unavailability of fund to purchase computer accessories in homes, offices and schools due to the high cost of E-learning infrastructures. | Bibiana, et al (2015) |
| Internet Connectivity, Inequality of access to the internet by students due to the land scape and unavailability of network provides in some riverine area, School Curriculum, Attitude of Students, Software and License cost, and Electricity. | Stephan (2012) |
| No training and re-training programs for teachers with respect to developing of their ICT skills at the minimum least stage of education in Nigeria (such as Basic schools and secondary schools). | Timothy et al (2008) |
| Limited expertise for Maintenance and Technical Support | Oye et al (2011) |
| Unavailability of skilled personnel at various levels of education, unavailability of ICT facilities, and learner's location are some crucial factors affecting learning for students from lower socio-economic background like most students in Nigeria. | Clarke (2002) |
| Qualified teachers to teach ICT are limited or sometimes not available in schools, increased moral degradation and burglary | Torruam, (2012) |

Table 1:- Identified Studies Addressing Various E-Learning Issues in the Context of Nigeria Environment.

In spite several challenges/issues the E-learning system in Nigeria is encountering, the ministry of education together with some education coordinating agencies of government in Nigeria has presently nine ICT for education initiatives at various stages of educational development. These include;

- Nigerian Universities Network (NUNet) project
- Polytechnics Network (PloyNet) project
- School Net project
- Nigerian Education, Academic, and Research Network (NEARNet)
- 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.

Presently, some institutions of higher education in the country have started setting up their ICT centers but their main aim is not to engage in E-learning but just to set-up an internet facility.

## IV. E-LEARNING SECURITY ISSUES

E-learning gives students' numerable advantages like: increases their access to education, flexible time and place of class, availability of different learning resources like E-books, higher opportunities for personal 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 partners in the E-learning system. They are;

- 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 include text, audio, video, or power point presentation for online courses.
- Instructors: these are the tutors.
- Administrator: Administrator maintains the material on server and controls the services. Learner access the LOs through network (Internet).
- Learners: these are the students.

The relationship between the four partners is shown in Figure 1 below.

ISSN No:-2456-2165

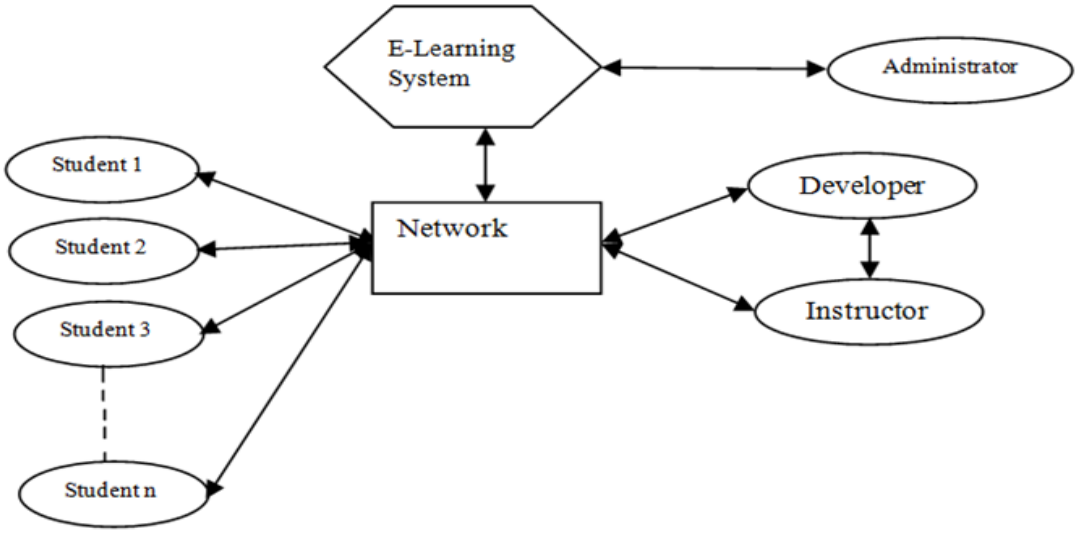


Fig 1:- E-Learning Access Model

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;

*A. Confidentiality Violation:*

Confidentiality can be described as protecting the assets of E-learning system from unauthorized access or user and modification. Confidentiality violation is a situation that occurs when an unauthorized user gains access to the facilities of the 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).

*B. 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 add or remove data. Integrity Violation can be seen as a process whereby an unauthorized user gains access and temper with an facility or document used in E-Learning system. Integrity depends on access control.

*C. 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 an essential factor of E-learning environment as it is a 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.

*D. Denial of Service:*

This is a situation that occurs when traffic interrupt prevents a person with legal access rights during a transaction to make use of the E-Learning system.

*E. 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 Illegal use or privilege Exploitation by legitimate users.

*F. Malicious Program:*

These are lines of code that can cause arm to other programs in the system.

*G. Availability:*

This refers to as the level to which the system is available for learners when neened Behkamal, et al, 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 a user is not capable to accessing the required material on time they may be frustrated or lose their interest.

*H. Traffic Analysis:*

This occur when a communication channel is abused and this situation results in information leakage.

*I. Masquerade:*

This is a way of behaving that seems to hide the true identity of an hacker(s).

## V. 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 is a mechanism that enables a person to include unseen copy right notice to video, audio and images. With this in place, the multimedia aspect of the E-learning system will be guarded from illegal users. Also, vital information like question papers, vital study material etc. is not visible to every viewer so chances of hacking is minimized to its barest minimum.

- *Access Control Using Firewall:*

Firewall is a mechanism that cones hardware and software security measures in other to stop an illegal user from outside an organization for gaining access into its corporate network. It combines packet filters and application gateways which has the potential of blocking traffic coming in but will allow E-learning users to communicate in and out freely from outside. The logic used in achieving this is that all in and out and vice vasa passes through the firewall. To achieve this logic, all access to the organization's local network should be blocked initially and all access should be channeled via the firewall. The traffic permitted only by the local security policy should pass through. It is the sole responsibility of the system administrator alone to have knowledge and skills to manipulate the firewall, to monitor and troubleshoot firewalls.

- *SMS Authentication:*

In Nigeria, the use of mobile phone is constantly on the rise. Presently, over one third of its population use cellular phone as compared to those using computer. As such, 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***:**

Learners must be comfortable to rely on the correctness of any content received from E-learning platform. Cryptography technique is one of the mechanisms that can offer privilege. The technique is off two types of algorithms in cryptography namely; Secret-key algorithms: In this technique, 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). And 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, 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.

## VI. 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 a major threat to E-learning system. If 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 quite 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 above to mitigate the security risk, though no system is absolutely secured. Moreover, the data transfer process to and fro should employ a combination of encryption techniques. A much secured learning system should not only incorporate security measure but also endeavor to keep the processes transparent and easier for teachers and 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.