Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1489–1498
DOI : 10.47974/JDMSC-1775

A study of e-learning security system and its impact on educators

Tanya Garg *
Ruchi Goyal †
Jaipur School of Business
JECRC University
Jaipur
Rajasthan
India

Dinesh Goyal §
Department of Computer Engineering
Poornima Institute of Engineering and Technology
Jaipur
Rajasthan
India

Abstract

E-Learning is the process of learning which includes interaction between teachers and learners, with comparison to traditional method of education. Plus, it is dependent on the web applications and internet technology. But, the environment of network is considered as a honey pot as it attracts many hackers; also, it is prone to many security risks like, malicious attacks, hackings, etc. Network security is one of the major concerns of the teachers, learners, instructors, etc., as they are not able to foresee risks and do not know the prevention as well. The aim of this study is to investigate the security issues associated with e-learning and effective countermeasures to prevent or mitigate these risks.

Subject Classification: *68M25.*

Keywords: *Security, E-learning, Teachers, Risks, Education.*

* *E-mail:* **tanyagarg.ag@gmail.com (Corresponding Author)**
† *E-mail:* **ruchi.goyal@jecrcu.edu.in**
§ *E-mail:* **dinesh.goyal@poornima.org**

1. Introduction

Technologies allowing natural modalities for entering information and instructions in hand-held devices are among the primary technical developments that have contributed to the flood of digital assistants in numerous sectors of a human being's activities and existence. As a result, the inclusion of written and spoken natural language acquisition and real-time comprehension has gradually expanded gadgets such as tablets, phablets, and smart phones into intelligent personal assistants such as Siri, Cortana, and Google Now. Taking advantage of human movement control models, we can imagine that in the near future, these pen-based hand-held devices will supplement people's sensitive data protection with automatic signature verification, equipment access security with writer authentication and handwritten CAPTCHAs processing (e-security), and human-machine interface through various gesture commands, word spotting, and handwriting recognition (e-recognition).

New education is often pigeonholed as modern education or transferring of digital technology into practicing of on-premise schools. Therefore, problems in technology of pedagogy unavoidably rises in schools and teachers' vulnerability. This procedure is momentously dominated by the transmission of organization structures of digital learning into environment of old-classroom learning. Furthermore, there is a definite type of intrusion in middle of educational long-established risks and IT- risks. For facilitating a suitable safeguarding, a standard of measurement and security models in digital learning are required.

2. E-Learning/ Digital Learning 2.0

E-learning, as we know it, has been around for around 10 years. At that period, it progressed from being a radical theory whose usefulness had yet to be shown to something widely accepted as mainstream. It's the cornerstone to several company ideas and a service given by most institutions and universities.

And now, e-learning is developing with the World Wide Web, and the changes are big enough to deserve a new name: E-learning 2.0. In the field of e-learning, the closest thing to a social network is a community of practise, which was articulated and pushed in the 1990s by people like Etienne Wenger.

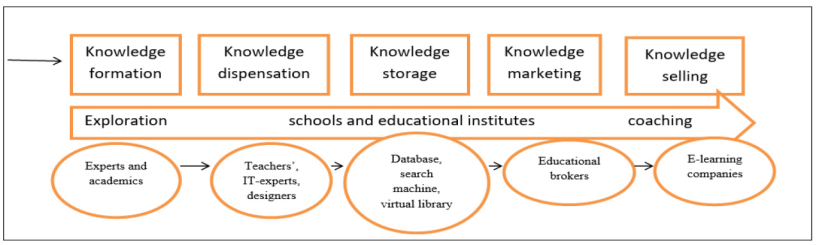
A determinist viewpoint holds that technology is all-powerful, capable of causing change regardless of the conditions. There are

curriculum and pedagogical approaches to educational technology that can improve digital learning for everybody. Such methods stress scaffolding in reading, writing, and cultural literacy while also offering access to new digital-era literacies; provide strong human supervision and mentorship from teachers and peers; and serve to connect in-school and out-of-school learning rather than devalue either (Sousa, M.J. and Rocha, Á., 2019). In e-learning, the way of interaction between teachers and students along with content of studying has been revolutionized in Web 2.0. Web 2.0 is similar to e-learning 2.0, where learning is facilitated through collaboration as well as sharing of content and ideas with learners.

The structures of e-learning 2.0 are as follows,

- Knowledge sharing
- User content
- Collaborative/ social/ network environment of learning

Knowledge flow of e-learning chain includes computers, by way of physical information collections and both internet and intranet as the medium of storage and communication. It is important to consider specific architecture of PLE (Personal Learning Environment) and VLE (Virtual Learning Environment). Teachers', IT-experts and multimedia designers are considered as actors (Figure 1).

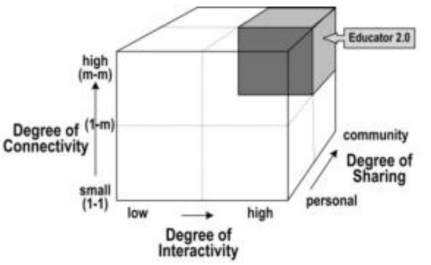


Source: Hilse, 2000

Figure 1

Knowledge management value chain

There are three dimensions of modern educator who are participants of online communities of education, namely- sharing, interactivity and connectivity. (Figure 2)



Source: Zuev, 2012

Figure 2

Educator's 2.0 online involvement degree

First dimension is educator's interactivity, as with more interaction of online users the process of education improves. The teachers' who are highly interactive considered as responsive; they usually reply to all e-mails on the very same day. They are also available through an online chat.

Second dimension is connectivity, it is important that all the team members are well connected so that they can respond according to the requirement without any delay. If a social network is wide as well as active then it is crucial to be connected for educational task. For better educational community, the connection of its member is necessary.

Third dimension is knowledge sharing and group connectivity, where the member shares their knowledge which gives quality of deliverables.

3. Virtual Learning Environment vulnerabilities and security policies of E-Learning

VLE are considered as integrated tools collection which enables online learning management, and gives tracking, delivery mechanism, an access to resources and assessment. The VLE of a university or schools should provide:

- Data protection
- Adequate resources for educational multimedia
- Accurate assessment of students'
- Learning objects reusability
- Feedback reliability
- Learning path flexibility for students'

These elements which are mentioned above are part of chain of educational technology and are prone to hacking attacks, unauthorized modification and educational assets destruction. It is important for the schools to resolve problems which are associated to plagiarism, authentication of student, copyright protection and unfair performance in assignment (Manadhata and Wing, 2010). So that the uprightness of teachers and smooth working of education system can be protected.

The policies of security of e-learning should be based on these assumptions:

- The focus should be on the protection from destructive as well as probable attacks;
- A continuous VLE control should be provided for revealing the unauthorized alterations;
- A rapid plus adequate response should be automated towards threats;

Meanwhile, e-learning security elements are the most common selection for handling integral problem. There are four basic security requirements for e-learning which are different from AIC triad of information security. They are as follows:

- In order to ensure privacy, it is required that the users have access to only those objects where he is permitted,
- For maintaining the uprightness of various assets, sanctioned users are allowed to adjust program and data,
- Accessibility of an efficient program for reducing attacks,

Typical threats to e-learning are as follows:

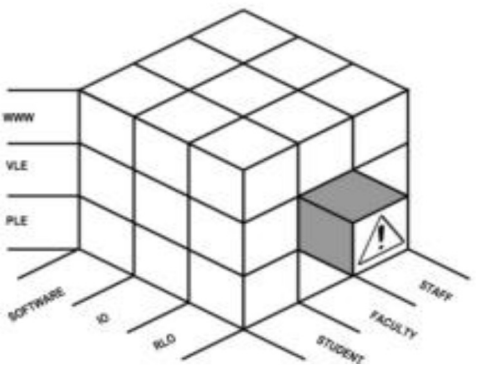
- Digital content unauthorized access which includes modification or copying of data or servers physical access,

Inadequacy and lost integrity of educational resources,

- Assessment procedure violation such as cheating, student identification, plagiarism, etc.,
- Hampering the usual functioning of e-working of various departments,
- Law violation like copyrights or other governing rights.

4. Aspects of security model of e-learning

Where e-learning is concerned, it is important to consider all the vulnerabilities and risks associated with it. Here in this particular case, this system is based on dualism i.e., subject of object. It made an strive to view dualism by a prism of e-learning cube (Figure 3 and 4).



Source: Zuev, V.I., 2012

Figure 3

Origin of VLE level software, attacks on faculty

Axes of model showcase the interaction level between teachers', VLE, students, global network, and various digital resources such as information object, software, objects of learning and elements of staff, students and faculty.

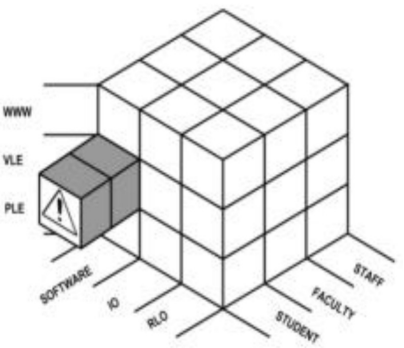
In figure 3 it is showed that the attack has been made on faculty at VLE level. Sources of threat originated from software which can be destruction, modification, alteration, etc. In figure 4, this situation has been reversed as the attack has been made on software at VLE level which is originated by the faculty.

Now will consider the didactic risks of system of e-learning. All these risks are mostly associated with faculty.

Firstly, risks which are associated with the expertise of the faculty are as follows:

- When the training course is not updated by the teacher is considered as didactic risk.
- ICT is not fully used by the teacher is technological risk.

- Scientific risk is educational material quality which is provided by teacher.
- Teacher shifting to LMS is delegation risk.



Source: Zuev, V.I., 2012

Figure 4

Attack on software at VLE level originated by faculty

Secondly, the risks which are associated with educational process of the organization, it is the result of insufficient control and improper planning of educational process including assessment and consulting activities. These risks sources draw origins to lacking cooperation among teachers, inadequate information system of student or subject disciplines.

Finally, the last risks are allied with faculty which has direct risk to process of education, which results in inappropriate behavior of student, the low professional responsibility of teacher and discipline breaching.

Perhaps, a large number of risks are concerned with students.

- First risk is of the inability of maintaining a learning rate.
- Second is the risk of constant motivation of student.
- Third is the risk of inadequate behavior and self- esteem of student.
- Fourth risk is inability to contact teacher.
- Lastly, the technological risk which has high competence of ICT among students.

There are other types of risks also present which are related to staff, that can be termed as subject or object of attack on the system of e-learning.

Hence, security system of e-learning metrics formalization as well as it is very difficult to create such as an adequate model.

5. Security Metrics of E- Educational Institutes

Metrics is considered as an effective tool for managing the security of university discerning effectiveness of different components of security of programs, specific LMS (learning management system), process, product and abilities of staff or faculty for addressing the issues of security for which they are considered responsible.

Safekeeping system of e-learning comprises analysis of:

- Topological analysis of system of e-learning construction,
- Intricacy accounting of software cyclomatic,
- Secretarial of enlightening as well as psychosomatic elements of educational process.

Meanwhile, there is a other convenient way of solving the problem. Any time when any attack occurs, the system of e-learning comes in contact with an attacker, which uses various information channels and imitates method sand ways of system, which results in receiving and sending of information from system. Same type of acts can be done by attacker while attacking on informational sites. Hence, methodology can be developed for such case.

"VLE attack surface" – is considered as possible vulnerabilities of security system of e-learning. These are- elements of LMS, techniques of e-learning, channels of data transmission, output and input of system, software, procedure, database, etc. If more components are there in VLE then there will be greater vulnerabilities and attacks.

Meanwhile, all elements in VLE are not the part of "VLE attack surface", those are exposed are considered unfit in breach potential. Consequently, it is required to prompt standards for retrieving the exposures.

VLE essentials becomes part of "VLE attack surface" if it is used by an attacker to disrupt usual performance of system. For assessing ability of element, it is reasonable to familiarize criteria which are based on ratio:

"[Cost of System Recovery/ Damage from attacker actions]"

Another possibility is assessment ratio including repair time of system and failure time of system. Therefore, "VLE attack surface" is an

important feature of system vulnerability as a total. It springs an idea of the damage can be caused by the attacker to the system and it also gives the notion regarding way of acting in command to damage an e-university at the same time.

The theory of "attack vector" was introduced by Manadhata and Wing (2004), it is a malicious disruption which affects the normal performance of the system. Hence, "attack vector" set can be defined as the risks and threat sets to e-learning system.

6. Conclusion

A satisfactory evaluation of risks and vulnerabilities of system of e-learning which will certify the model creation conferring to which an approach of fortification can be formed. Hence, modeling threat is an important part of planning system of e-learning. It is required to pay attention to issues at early stage of emergent secure system of e-learning. This will enable to analyze adequately architecture system for detecting and solving problems of security. This will provide extra security to the educators in schools.

References

[1] Zuev, V. I., E-learning security models. *Management Information Systems*, *7*(2), 024-028 (2012).

[2] Huu Phuoc Dai, N., Kerti, A., & Rajnai, Z., E-learning security risks and its countermeasures. *Journal of Emerging research and solutions in ICT*, *1*(1), 17-25 (2016).

[3] Baby, A., & Kannammal, A., Information security modelling in an e-learning environment. *International Journal of Computer Science Issues (IJCSI)*, 11(1), 195 (2014).

[4] Weippl, E. R., *Security in e-learning* (Vol. 16). Springer Science & Business Media (2006).

[5] Di Martino, B., Cretella, G., & Esposito, A., Semantic and agnostic representation of cloud patterns for cloud interoperability and portability. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, Vol. 2, pp. 182-187 (2013, December). IEEE.

[6] Howard, M., Pincus, J., & Wing, J. M., *Measuring relative attack surfaces* (pp. 109-137). Springer US (2005).

[7] Manadhata, P., & Wing, J. M., *Measuring a system's attack surface*. Carnegie-Mellon Univ Pittsburgh pa School of Computer Science (2004).

[8] Manadhata, P. K., & Wing, J. M., An attack surface metric. *IEEE Transactions on Software Engineering*, 37(3), 371-386 (2010).

[9] Garg, T., & Goyal, R., A Comparative Study of E-Learning Applications. In *Proceedings of the Third International Conference on Information Management and Machine Intelligence: ICIMMI 2021*, pp. 635-645 (2022, August). Singapore: Springer Nature Singapore.

[10] Garg, T., & Goyal, R., Evolution of education system and techniques: A comparative study. In *Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020*, pp. 755-763 (2021). Springer Singapore.

[11] Zakia, R., & Yana, D., English Teachers' Perception of Security in Digital Literacy Competence. *Journal on Education*, 5(3), 8873-8882 (2023).

[12] Singar, A. V., & Akhilesh, K. B., Role of cyber-security in higher education. *Smart Technologies: Scope and Applications*, 249-264 (2020).

[13] Susila, N., Sruthi, A., & Usha, S., Impact of cloud security in digital twin. In *Advances in Computers*, Vol. 117, No. 1, pp. 247-263 (2020). Elsevier.

[14] Atanasov, V., & Ivanova, A., A FRAMEWORK FOR EVALUATION OF WEB BASED LEARNING CONTENT. *International Journal on Information Technologies & Security*, 14(4) (2022).

[15] Duodu, N. Y., & Patel, W., Advanced EHR system in homes-in-schools' automation using internet of things and machine learning. *Journal of Information and Optimization Sciences*, 43(8), 1953-1962 (2022).

[16] Khan, S., Tailor, R. K., Pareek, R., Gujrati, R., & Uygun, H., Application of Robotic Process Automation in education sector. *Journal of Information and Optimization Sciences*, 43(7), 1815-1834 (2022).