|| Volume 6 || Issue 8 || August 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

E-LEARNING PLATFORM SECURITY ISSUES AND THEIRPREVENTION TECHNIQUES: A REVIEW

Priyanka Sharma — CEA Dept, GLA University

Kirti Agarwal — CEA Dept, GLA University

Priya Chaudhary — CEA Dept,Gla University

Abstract: E– learning(EL), nowadays a most popular means of learning and also a major platform for interaction between teachers and students . Online web platform and network environment are the major source for e-learning. So, tremendoususe of online learning software over internet arises the need for protection. It has as well become the dearest thing for hackers, who gain access to these platforms by unethical ways. This study is carried on to explore the security issues on the e -learningplatform and also suggest some prevention techniques for these issues

Keywords : E-learning(EL), information security, informationand communication technology

I. INTRODUCTION

E- learning (EL) offers the scholar-specified location that students can take the course all over. Because with the new technology, the courses are stored on the web applications and accessible 24 hours per week. They can use their multi-devices as laptops, computers, smart phones and so onin order to approach the course everywhere. They don't needto go to school at a particular day in a week. Besides , they can read, download online materials, learn the courses and update the cognition agilely(Huu Phuoc Dai et al., 2016) .

An enormous outgrowth of information and communication technologies (ICTs) has positively touched the field of EL. Lately the teaching mode is changed over from the traditional classroom towards EL. With the marvelous growth of Internet technologies and computing, EL continues to prove its Magnificence, and has started to have the same report as Traditional learning methods. Thus, countless studies have shown that e-learning has been growing and is widely used all over the Universe. Some cyber security issuesassociated to e-learning system such as corrupted or lost communications, messages, grades, data or work; a compromised the user and the teacher identity; stolen personal information and corrupted social technical systems. Therefore, we need to guarantee the security and the safety ofthe users in the e -system.(Huu Phuoc Dai et al., 2016)

E-learning emerged from the traditional/classroom learning in the late eighties and nineties leveraging the power of ICT and computing. The use of ICT and the internet in learning gives e-learning edge over traditional classroom methods. However, due to deficiencies of the e-learning inthe areas of cost and time disadvantages as well as the advancement in Internet technologies (leading to emergence of cloud computing), the world is witnessing a shift in the usage of e-learning to mobile learning (m-learning). M-learning is a term that denotes the delivery of learning materials and other content through the use of mobile devices that can easily be accessed anywhere in the world (Adejo et al., 2018)

Blended learning is an approach to education that combines online educational materials and opportunities for interaction online with traditional place-based classroom methods. It requires the physical presence of both teacher and student, with some elements of student control over time, place, path, or pace.

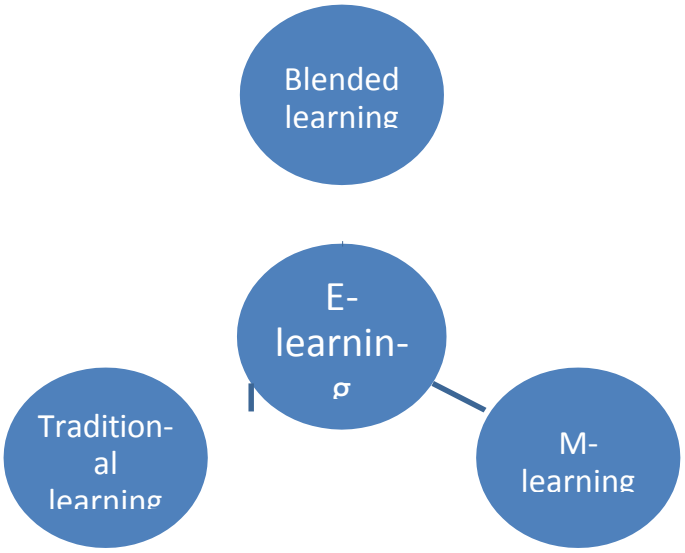

Figure 1: E-learning Model

E-learning solutions are scalable where the programs can have more participants with low cost. It is the effective way to provide the information as it reduces the travel expense, teaching time and physical need for a teacher and classroom infrastructure. The system can enable learners to be integrated and form learning communities by creating knowledge society and sharing knowledge .(Alghamdi, 2018)

|| Volume 6 || Issue 8 || August 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

ELearning Platform Security Issues and Their Prevention Techniques:A Review

The purpose of this paper is to briefly analyze the related discussions in the literature review, to provide a summary review of the security aspects of the e-learning management system, and also to discover the security challenges in an e-learning management system.

The study embraced different techniques in reviewing the cyber risk involved in an e- learning management system, through a detailed literature review using academic databases, secondary sources such as Google Scholar and journal research papers. This paper aspires to organize this information to help Administrators, students, researchers and educators to know the risk involved in an e-learning management system. And hence, implement some security measures to provide a secured and protected environment for e-learners against cyber attacks.

II TRADITIONAL LEARNING Vs E-LEARNING

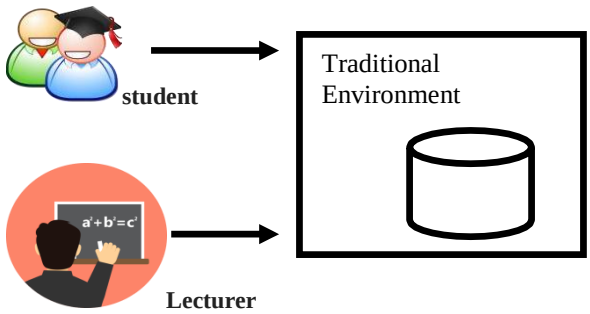

Figure 2: Traditional Learning Environment

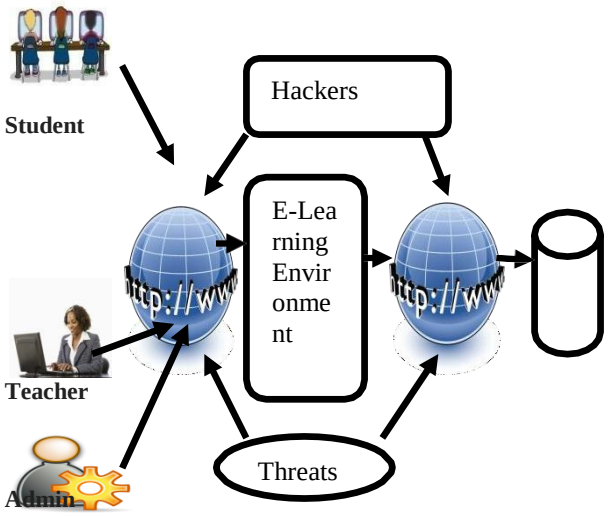

Figure 3: E-Learning Environment

TRADITIONAL LEARNING	E-LEARNING
Consist of central physical environment	Consist of online environment
Infrastructure Required	No Infrastructure required
No flexibility in timing , everything should take place at appropriate fix time limit	Flexibility in timing , student can learn any time day or night
Closed system environment , information security threats can be kept minimum	Open access environment ,highly exposed to security threats
Learning materials should be delivered through books , hard copies ,notebooks , blackboards and smart boards .	Learning materials delivered through softwares , pdfs , docs, files, soft copies etc by online mode
Teachers , students and information present at the same physical location	Teachers , students and information present at different geographical location
Information security risk is less as it is limited to single physical place	Information security risk is high and could be compromised

Table I- Traditional learning Vs E-Learning

III PROBLEM DESCRIPTION

Recently, E-learning system has faced some concerns related to security, availability, and reliability due to covid crisis . All educational institutions , coaching institute had take their move towards E-learning immediately. To overcome these challenges, a significant security framework is required to protect the data involves approach of e-learning system. It is important to ensure the security and privacy of e-learning data which needs a consistent framework to avoid the security issues . So, In this paper a systematic and quality review of papers related with security issues of E-learning platform and their prevention techniques , potential threats etc were done and literatures gaps were found out. This paperis helpful for those who want to do further research in the field of E-learning system security .

III RELATED WORKS

Many researchers have majorly talked about main security issues like Confidentiality , integrity , Availability , Authorisation , Authentication ,data privacy and their counter measures . Some of the researchers have proposed various cloud based architecture and some other have described about various cryptographic schemes like Identity based broadcast encryption (IBBE) , Cipher text policy Attribute based encryption schemes (CP-ABE) . Some authors described about various types of active and passive attacks ,threats and vulnerabilities .

(Humayun, 2020). In this paper the author had discussed about selection of good E-learning tools which are useful for E-learning practitioners in the time pandemic which is a necessity of today. Also provided E-learning framework for the privacy and security of E-learning data and environment . The author had gathered real time statistics and analyzed to envisage the impact of COVID-19 on education around the world. The increasing demand for EL during COVID-19 is analyzed, and a complete catalog is provided to make the EL practitioners aware of existing distance learning solutions. A comparison of commonly used EL tools is provided that will help in the selection of EL tools according to institutional requirements. A Blockchain-based EL framework is proposed that will help EL designer in managing the security of EL data and environment . The proposed framework is expected to provide a promising solution for developing a fair and open learning online education environment and will overcome the deficiencies caused by school closures during COVID-19.

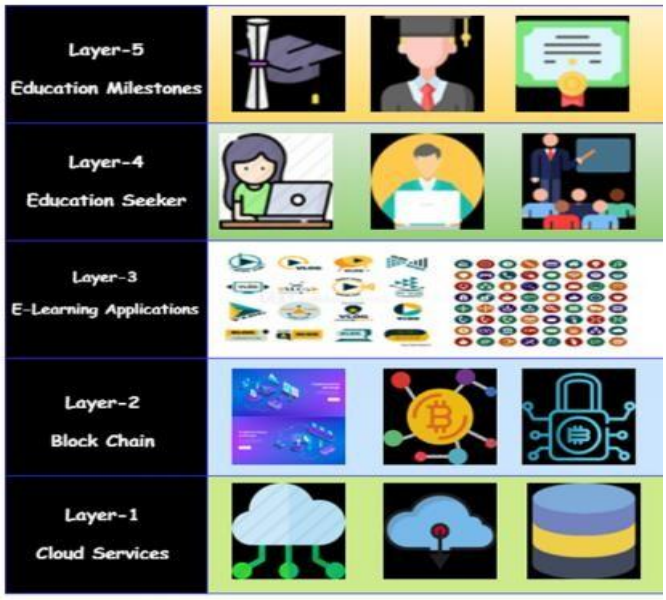

Figure 4: Block chain based E-learning framework(Source : (Humayun, 2020)

(Ben Amor et al., 2020) In this paper, a new fog computing e-learning scheme is proposed. Specifically, the proposed solution extends learning content from the cloud to the edge of the network. It can improve the efficiency of learning data analysis, reduces the encryption burden in terms of computation cost on user's devices by offloading part of encryption cost to fog servers and provides fine grainedaccess control to learning content by encrypting the course and the exam with different cryptographic techniques like IBBE and CP-ABE . Further, the author presented a profile matching mechanism that helps teachers to find colleagues within their vicinity in an efficient and secure way. Security analysis shows that this scheme can achieve data confidentiality, fine-grained access control, collusion resistance and unforgeability. Performance evaluations demonstrate the efficiency of this solution, especially in terms of encryption computation.

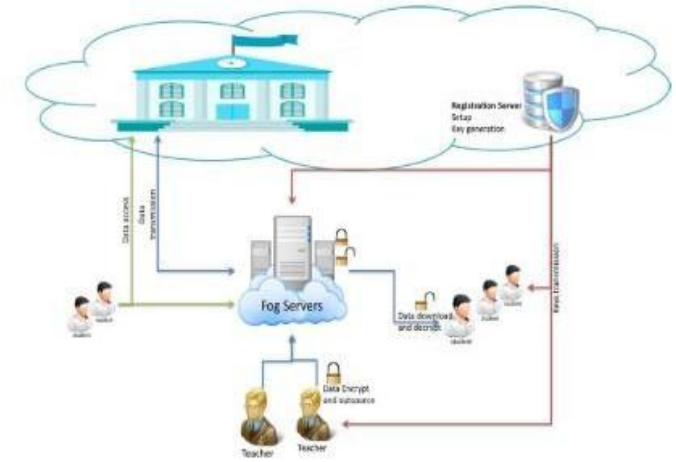

Figure 5 : Secure Fog Based E-learning Architecture(source: (Ben Amor et al., 2020)**)**

(Adejo et al., 2018) In this paper authors discussed the various advantages of the using m-learning platform and cloud infrastructure in higher education. It also examined the vulnerabilities of the platform as well as other security and privacy challenges regarding the effective implementation of m-learning in cloud infrastructure environment. Finally, The authors proposed a detailed data protection and security framework that is needed for addressing these issues. It is desired that the proposed framework when fully implemented, will bring about necessary solution to issues related to the security and data protection of m-learners in cloud computing environment, increase faith in the use of the system as well as enhance the m-learning platforms.

(Ivanova et al., 2015) In this paper author presented data privacy model created after explorations related to the measures for security of private information in different online transactional fields including in the area of eLearning and after results summarization of students' opinion. The findings shows that privacy in eLearning could be achieved through a combination of actions from student's side, third parties' side and appropriate design of educational software

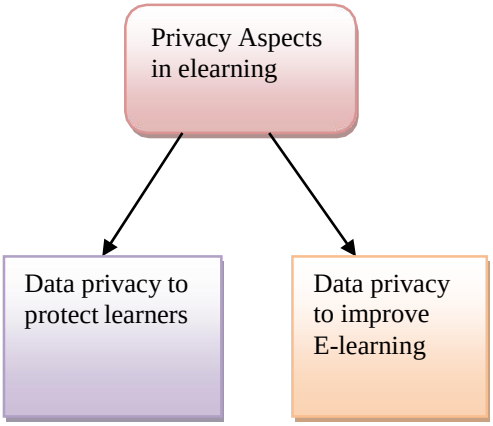

Figure 6: Privacy Aspects in E-learning(Ivanova et al., 2015)

Student side 1.what information share 2.what relationships make 3.how his computer / mobile device is protected	**Third Parties side University** – keeps and shares just needed data with students' agreement, secure information system and databases -**Educator** – operate with minimal personal data, knowing of learning preferences, styles, learning progress -**Other students** – use the shared data -**Administrator** – indirect involved, keeps private data	**Educational software-** Ensuring anonymity -Tools for sharing on trust -Options for choice of sharing -To educate in privacy -To give hint when much data are shared -Password protection -other technical issues
Privacy in E-learning		

Figure 7: Data Privacy Model in E-learning (Source:(Ivanova et al., 2015)**)**

(Savulescu et al., 2015) This paper presents a model of security for the implementation of the e-learning system, partly verified during the implementation at the universities in Romania and Poland . It presents the results for the crossovers between some technological fields, such as e-learning and the standards to improve security systems in education. Universities, schools and other kinds of organizations are choosing more and more often the e-learning platform to offer on-line education. In order to achieve the research objectives, the following questions have been formed by the author

- What kind of threats are their in E-learning?
- How can the E-learning system can be secured?
- Which model of security dedicated for E-learning system could be optimal?

Inorder to answer first question : The theoretical framework of using e-learning systems to characterize the kind of threats was examined

The answer to second question was achieved by comparative analysis of available e-learning systems was carried out.

the last question was answered by presenting the findings and then the implications and recommendations of the research, with pre-determined and defined areas of secured e-learning models . Solutions given by the author such as UTM (Unified Threat Management), Firewalls, biometric authentication, data storage or face recognition system.

(Alghamdi, 2018)In this paper author asserted about cloud computing as the emerging technology in the field of education . Author discussed about the significant security challenges like reliable, availability and security found in

E-learning using cloud technology. Author also Proposed a cloud service delivery model and web 4.0 for avoiding the challenges in the eLearning and enhance the efficiency of the system. Furthermore, the proposed model provides possible solutions to the e-learners and educators forusing the system efficiently . This integrated model canreduce the issues of data security and data availability in the eLearning system using cloud computing.

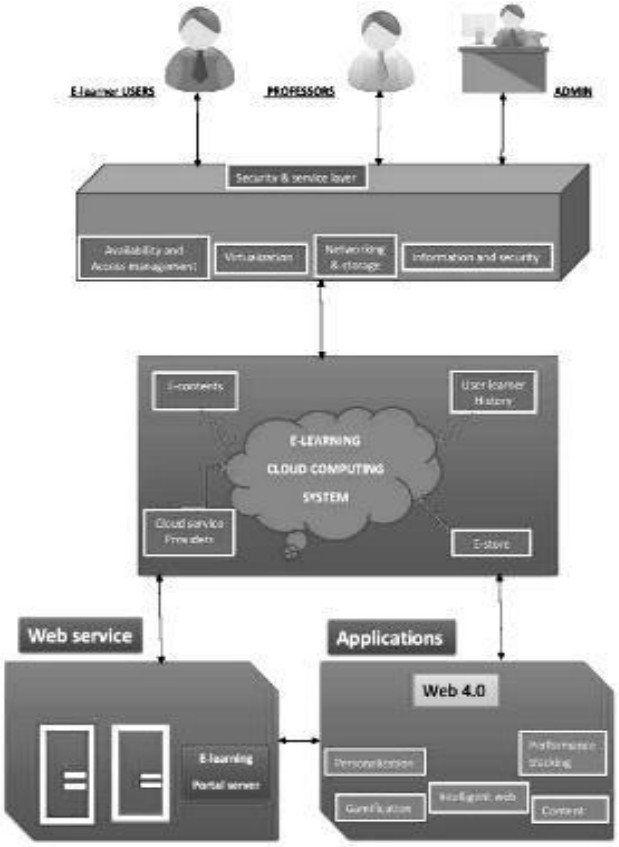

Figure 8: Integrated cloud model for intelligente-learning system((Alghamdi, 2018)

(Jahankhani et al., 2016) In this paper authors identifies the causes of privacy concerns which emerged when an educational institution launched an automated proctoring technology to examine E-Learners.In the modern times of information, privacy is an integral concern due to its fluid, dynamic and complex nature. In certain conditions where it is very difficult to understand the privacy concerns, privacy is often misunderstood by the interactive systems designers.

A tracking tool called Proctortrack was launched for students which lead to many privacy and security concerns while providing online proctoring services. This proctoring tool was designed to monitor the student's behavior and find out if the user is a legitimate student. A webcam was fitted within the Proctortrack services capturing facial features of students for the verification purposes and being sensitive to their movements which may lead to any misconduct or cheating .

(Neena et al., 2016) In this paper authors discussed about the problem of copying of video file of lectures upload by educators in the repositories of E-learning system through internet . Authors asserted that it is not so difficult to copy such video files without quality loss. So,In order to protect these vedio files author come up with digitalwatermarking as strong solution for this problem. Authors proposed a method for digital watermarking in which frequency domain transforms (Discrete Cosine Transform (DCT), Discrete Fouriern Transform (DFT), Discrete Wavelet Transform (DWT)) were used for the data insertion. The decoding is based on the side information which produced at the time of watermarking.Comparision was done between the Peak signal-to-noise ratio (PSNR) and Bit Error Rate (BER) of the results. During testing applied spatial attacks and compression attacks on the watermarked video. The result shows that the method using wavelet transform is more efficient.

Authors proposed 3 methods for video watermarking. The first method uses 2D DCT to embed the watermark,second method used 2D DFT and in third method 2D DWT was used Then PSNR and BER of watermarked video calculated to evaluate the efficiency of the watermarking. Also checked robustness of the watermark system by attacking the watermarked video. And the results show that the 2D DWT method had more robustness against various attacks.

Figure 9 (a) Input video frame, (b) output of 2D DCT, (c) output of 2D DFT, (d) output of 2D DWT ((Neena et al., 2016)

To evaluate the transparency authors calculated the PSNR between original and watermarked video. It is shown in the figure.10 . High value of the PSNR is an indicator that the watermarked video is very similar to the original one, and hence the watermark is not visible. Here 2D DWT algorithm has high PSNR value in comparision to other two methods .So the watermark is invisible. The PSNR value of 2D DFT very less and the watermark is visible in the frames of the video.

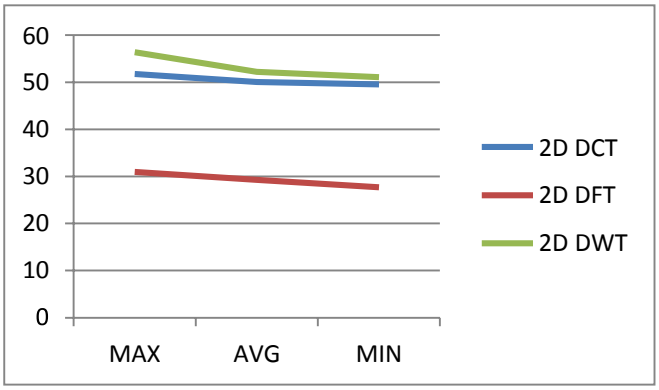

Figure 10: The above graph shows PSNR values of Tranform method (Source table from : (Neena et al., 2016)

The PSNR value of corresponding wavelet family is given in the figure 11. The result shows that any wavelet family can be used because all gives high PSNR values and the method will be transparent.

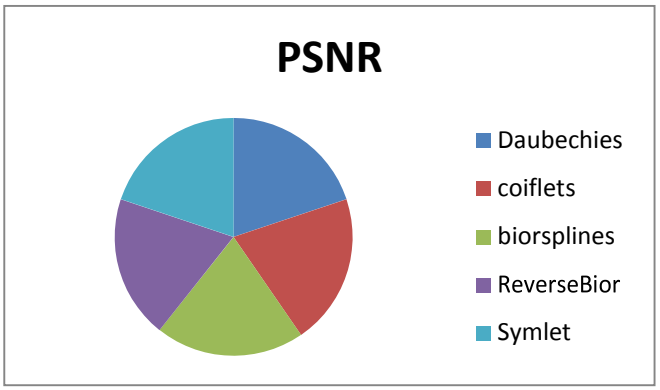

Figure 11: The PSNR values of 2D DWT algorithm using different wavelets (Source table from : (Neena et al., 2016)

(Chithra & Kalaavathi, 2015)In this paper author addressed the authentication of E-learning User as the security issue .So, usage of proper communication network for providing internet connectivity is another major challenge. WiMAX networks provide Broadband Wireless Access through the Multicast Broadcast Service so these networks can be most suitable for E-Learning applications. The authentication of E-Learning user is vulnerable to session hijacking problems. The repeated authentication of users can be done to overcome these issues. Author proposedsession based Profile Caching Authentication scheme. In thisscheme, the credentials of E-Learning users can be cached atauthentication server during the initial authentication throughthe proper subscriber station. The proposed cache based authentication scheme performs fast authentication by using cached user profile. Thus, the proposed authentication protocol reduces the delay in repeated authentication to enhance the security in E-Learning.

ELearning Platform Security Issues and Their Prevention Techniques:A Review

(Ayyad et al., 2016) In this paper, author presented an analysis of web application vulnerabilities like SQL Injection Attack, Cross Site Scripting and brute force login attack. some experiments were conducted by author using modern operating system kali Linux and also provided some recommendations and solutions.Author has taken two E-learning platform in consideration which are MOODLE and Word Press. WordPress is a tool for creating E-learning content using appropriate WordPress plugins .Author had shown this system as vulnerable due to SQL injection Attack and error in PHP code etc . Moodle developers treat security issues very seriously namely, vulnerabilities studied in this report were SQL injection attack , cross site scripting ,brute force login attack etc .So ,author has given some recommendation to minimize chances of these attacks . Kali Linux operating system used to understand some aspects of security of e-learning platforms and, analyzed the most important problems of an open source software WordPress/MOODLE.

(Huu Phuoc Dai et al., 2016) In this study authors mainly focused on E-learning security issues and the countermeasures to deal with risks towards e-learning-system. The online survey has been initiated by author and circulated (via Facebook groups) among studentsin Vietnam. The online quantitative survey consists of 24 questions on required fields. Based on the collective results author has formed three hypothesis

H1: E-learning system is very essential not only for full-time students but also for part-time and distance students in their training program.

H2: Web materials are valuable sources for all training students.

H3: Video materials are very necessary for all students during their training program.

Authors used Chi-Square test by SPSS to evaluate the correlation of the variables hypothesises in H1, H2, H3 in respectively. Authors had also discussed about various Counter measures to ensure security of E-learning like intrution detection system ,firewalls , secure protocol (HTTPS) ,Hash and digital signature algorithm , encryption techniques etc . The researchers strongly believed thate-learning will become more popular in the future and cryptography is the efficient and secured way to make the users feel comfortable and secure.

(Kritzinger et al., 2006) Authors asserted the difference between E-learning and Traditional environment . They identified technical and non-technical information security counter measures that could improve the security of information within the educational environments.There are six technical measures identified by the von solms :

- Identification and Authentication
- Authorization
- Confidentiality
- Non – repudiation
- Availability
- Integrity

Four Procedural counter measures identified by the authors were as follows:

- Ensure Information Security Governance
- Implement an E-learning Information Security Policy
- Establish an E-learning Security Risk Management Plan
- Proper Monitoring of Information Security measures

These counter measures should not only be adapted inE-learning environment but also be implemented .

(Ullah et al., 2016) In this paper authors have done survey of literature to present a threat classification using security abuse case scenarios. Authors asserted that Collusion as one of the challenging threats, when a student invites a third party collaborator to impersonate or help him/her in an online test. It is important to lessen all these types of attacks .So,the risk of collusion is increasingly challenging because it is difficult to detect such type of attacks. Collusion threats are motivated by vulnerabilities in identity and the authentication model. These threats were classified into impersonation and abetting. Impersonation happens, when a student willingly colludes and shares access credentials with a third party to commit impersonation. Abetting happens when a student takes an online examination assisted by a third party based inthe same location or remotely. It is difficult to track collusionattacks when an online test is completed. However, it is important to lessen such attacks in order to increase confidence of stake holders and improve the credibility of online assessment.

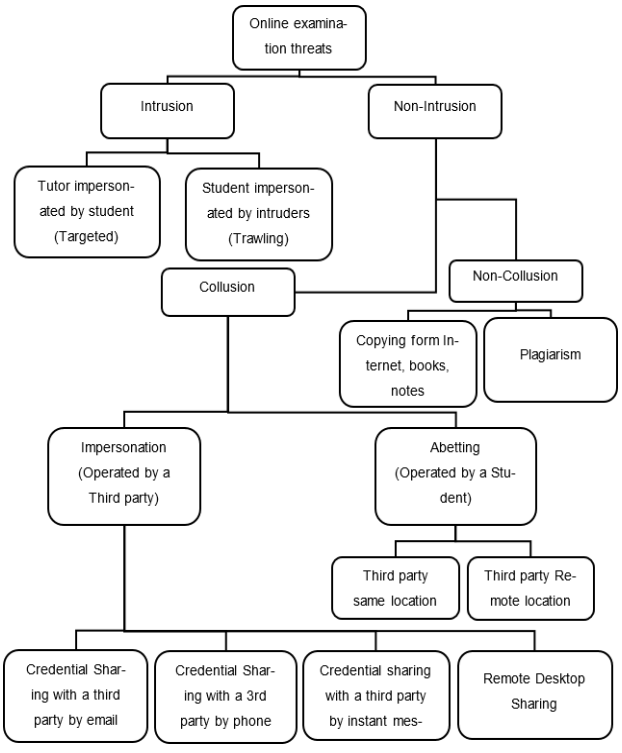

Figure 12 : Threats Classification (source : (Ullah et al., 2016)

Article	Type of Algorithm /Technology/Threats	Models, Frameworks, Concepts Discussed	Observations/Findings
(Kritzinger, 2006)	Technical and Proceduralcounter measures	CIA triad(Confidentiality, Integrity and Availability);countermeasures;	Some security policy measures and risk management techniques need to be addressed and implemented
(Ullah et al., 2016)	Collusion threat , Impersonation and Abetting	Classified threats on the basisof security abuse case scenario	Strong authentication mechanism and remote proctoring can be used
(Humayun, 2020)	Block chain Based E-learning framework Cloudservices and Block chain technology for security	A proposed Block chainbased E-learning model E-learning Tools used during Covid-19	Block chain technology is secured, but very new to the education field and also not budget friendly to be implemented everywhere.
(Ayyad et al., 2016)	Moodle and word press, SQL injection attack , XSSattack , Brute force login	Kali modern operating system based on GNU/LinuxDebian	Recommended configurationfor Moodle platform:- Web Server:Apache Security Server: OpenSSLDatabase: MySQL PHP pre-processor Strong passwords The latest version of MOODLE
(Huu Phuoc Dai et al., 2016)	Malicious , authentication , availability attacks DOS attack , Trojan and viruses ,stolen keys and passwords	Authentication ,Availability , integrity, confidentiality	IDS or Firewall can be used , biometric authentication, hash and digital signature algorithm can be used
(Chithra & Kalaavathi, 2015)	Authentication protocol likePrivacy Key Management Protocol (PKM V1 ,PKM V2) , NS3 simulator	Proposed session based Profile Caching Authentication	Proposed protocol can be enhanced by minimizing the number of messages exchanges during each reauthentication process.
(Neena et al., 2016)	Digital water marking Technology ,Frequency domain transform methodapplied	Vulnerability testing is done using spatial and compression attacks on water marked video	Wavelet transform method ismost efficient
(Ivanova et al., 2015)	Privacy aspects in E-learning ,Measures to protect user's privacy	Data privacy model inE-learning	privacy in eLearning could be achieved through a combination of actions fromstudent's side, third parties' side and appropriate design of educational software.
(Savulescu et al., 2015)	Unified threat Management system (UTM),Bio-metric authentication ,face recognition , Eye pattern recognition ,detectblinking eyes	Hybrid approach security of E-learning Finger print device , camera , smart phone	This model can be implemented in onlineE-learning Platform

(Ben Amor et al., 2020)	User Fog cloud based Architecture IBBE , CP-ABE cryptographic techniques	proposed a secure data sharing and profile matchingfog-assisted scheme for e-learning data system.	Scheme can achieve data confidentiality, fine-grained access control, collusion resistance and unforgeability
(Adejo et al., 2018)	M-learning and cloud infrastructure Authorisation,backup and	Proposed multilayer platform architecture for	Reccomended to adequately addresss security issues and

	recovery,encryption ,audit trail	data protection and security	data protection of m-learning on cloud platform
(Alghamdi, 2018)	Cloud based architecture Web 4.0 intelligent web	proposed integrated cloud model for intelligent eLearning system ; Virtualization ; centralized data storage	advanced version of web 5.0 in web-based education can be used in future work
(Jahankhani et al., 2016)	Online verification tool Webcam captures Facial features	Proctortrack tracking tool is used to find legimitate user	need for a robust framework for the awareness of all stakeholders where novel technology is used in untested scenarios.

CONCLUSION

The purpose of this review was to view the security issues and advancement in E-learning systems or environment within the past ten years . In this pandemic time as every educational institution is dependent on E-learning systems for conveying their study material and vedio lectures to the learners in easy accessible manner . So , there is need of good quality and secured E-learning platform. It is clear from the research review that (Kritzinger, 2006) , (Huu Phuoc Dai et al., 2016),(Chithra & Kalaavathi, 2015), (Ben Amor et al., 2020)have focused on CIA triad (Confidentiality , integrity and availability) . (Kritzinger, 2006) proposed Technical and procedural countermeasures to these security issues. (Ivanova et al., 2015)proposed hybrid security models or Data privacy models and suggested the use of latest securitytechniques like biometric , Firewall , Intrusion detectionsystem ,Proctortrack tracking tools etc . Within past ten yearsreviewed researches only (Humayun, 2020) have discussed about block chain technology and also proposed a E-learrning model using block chain . The author has also recommended for the real time implemention of the model .Although the block chain technology is very lastest and mostsecured technology than the previous ones but it require little more efforts to be implemented and adaptable by every educational institution for E-learning purpose . Future researchers are recommended to do more focus in this blockchain technology area .So that a better security platformcan be prepared for the E-learning purpose .

(Adejo et al., 2018), (Alghamdi, 2018) , (Ben Amor et al., 2020)have focused on Cloud based architecture which is also a very effective technology in this modern era . It is having so many benefits like speed , great accessibility , lower cost ,better disaster recovery and security . But it needslittle more focused in the field of E-learning as very less researchers have focused towards this. It will be helpful for the educational institutions and coaching centers to make their E-learning platform easily accessible and more secured . Some researchers have also described about threats and vulnerabilities in the learning management system and recommended some configuration to lessen the effect of these threats . Some more better countermeasures can be usedother than mentioned by the (Kritzinger, 2006) .So, thatE-learning system can be protected from these harmful threats.

Content analysis could be augmented with quantitative methods by sending a questionnaire to learners , educators and administrators in an attempt to confirm some of the results of the analysis of this study. A quantitative approach could fill some of the gaps and address the limitations on reliability and generalizability intrinsic in the contentanalysis approach adopted by the above study. On the other hand keeping within the qualitative standard, indepthinterviews could be arranged with E-learning platform users to explore deeper into the concerns and challenges that they face in using the E-learning system. Finally, for those who are interested in open source 'process' and e-learning security issues, there remains much research to be done

REFERENCES

Adejo, O. W., Ewuzie, I., Usoro, A., & Connolly, T. (2018). E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure. *International Journal of Information Technology and Computer Science*, *10*(4), 1–9. https://doi.org/10.5815/ijitcs.2018.04.01

Alghamdi, F. A. (2018). *An Integrated Cloud model for intelligent E-Learning system*. *13*(14), 11484–11490.

Ayyad, Y., Magrez, H., & Ziyyat, A. (2016). *SecurityConcerns in a Web-Based E-learning Platform Security Concerns in a Web-Based E-learning Platform*. *FEBRUARY*.

Ben Amor, A., Abid, M., & Meddeb, A. (2020). SecureFog-Based E-Learning Scheme. *IEEE Access*, *8*, 31920–31933. https://doi.org/10.1109/ACCESS.2020.2973325

Chithra, R., & Kalaavathi, B. (2015). *Secured Session Based Profile Caching for E-Learning Systems Using WiMAX*

Networks. *9*(6), 1618–1621.

Humayun, M. (2020). Blockchain-Based secure framework for e-learning during COVID-19. *Indian Journal of Science and Technology*, *13*(12), 1328–1341. https://doi.org/10.17485/ijst/v13i12.152

Huu Phuoc Dai, N., Kerti, A., & Rajnai, Z. (2016). E-Learning Security Risks and its Countermeasures. *Journal of Emerging Research and Solutions in ICT*, *1*(1), 17–25. https://doi.org/10.20544/ersict.01.16.p02

Ivanova, M., Grosseck, G., & Holotescu, C. (2015). Researching data privacy models in eLearning. *2015 International Conference on Information Technology Based Higher Education and Training, ITHET 2015*, *00*(c). https://doi.org/10.1109/ITHET.2015.7218033

Jahankhani, H., Carlile, A., Emm, D., Hosseinian-Far, A., Brown, G., Sexton, G., & Jamal, A. (2016). Global Triumph or Exploitation of Security and Privacy Concerns in E-Learning Systems Asim.

Communications in Computer and Information Science, 1, 351–363. https://doi.org/10.1007/978-3-319-51064-4

Kritzinger, E. (2006). Information security in an e-learning environment. IFIP International Federation for Information Processing, 210, 345–349. https://doi.org/10.1007/978-0-387-34731-8_42

Neena, P. M., Athi Narayanan, S., & Bijlani, K. (2016). Copyright Protection for E-Learning Videos Using Digital Watermarking. Proceedings - 2015 5th International Conference on Advances in Computing and Communications, ICACC 2015, 447–450. https://doi.org/10.1109/ICACC.2015.74

Savulescu, C., Polkowski, Z., Cosmin, D. I., & Elena, B. C. (2015). Security in e-learning systems. Proceedings of the 2015 7th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2015, WE19–WE24.

https://doi.org/10.1109/ECAI.2015.7301225

Ullah, A., Xiao, H., & Barker, T. (2016). A classification of threats to remote online examinations. 7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, IEEE IEMCON 2016.

https://doi.org/10.1109/IEMCON.2016.7746085