March - April 2020
ISSN: 0193-4120 Page No. 10471 - 10478

# Security Standards: Quality Parameter for E-learning Platforms

Swati Kirange[1], Dr. Deepali Sawai[2]
[1]Research Scholar, IICMR, Pune
[2]Director, IICMR-MCA, IICMR, Pune

***Article Info***
***Volume 83***
***Page Number: 10471 - 10478***
***Publication Issue:***
***March - April 2020***

***Article History***
***Article Received****: 24 July 2019*
***Revised****: 12 September 2019*
***Accepted****: 15 February 2020*
***Publication****: 13 April 2020*

***Abstract***
E-learning is referred as learning with the help of information and communications technology to access educational curriculum outside the traditional classroom. E-learning is widely accepted in higher education. Internet itself is considered to be insecure so it becomes difficult to protect resources shared through network. Providing secure environment is necessary to build trust in the minds of users of online learning system. This study highlights different security threats and attacks possible on e-learning systems. This article suggests the need of tracking student activities in online teaching-learning process. Authors have discussed various countermeasures to the security issues.

***Keywords:*** *E- learning, standards, security, threats, measures.*

## I. Introduction

In recent years there is drastic increase in number of e-learning platforms used by schools, colleges and corporate. E-learning is defined as the use of electronic media and information and communication technologies in delivery of education. All the forms of educational technologies for teaching-learning process are incorporated in online learning systems. Online learning platforms provide robust, secure and integrated personalized learning environments that could be used by learners, teachers and administrators. E-learning composed of multimedia learning, technology-enhanced learning, computer-based instruction, computer-assisted instructions, web based training, virtual learning environments and mobile learning [1]. These technologies include audio, video, blogging, whiteboard, screen casting, virtual classrooms etc. Recent technological development incorporates adaptive e-learning, personalized learning and games as part of learning [2].

Web based e-learning systems are more vulnerable to security issues arise through internet. These issues include denial of service, malicious programs, masquerade attack, violation of confidentiality, integrity, availability, authorization, authenticity of information etc. The use of interactive platforms and multimedia tools makes learning content delivery as valuable and more appealing for the users. With the advent of cloud technology on demand e-learning systems are widely adopted. These systems reduce cost and data accessing complexity but compromises on security aspects [3]. According to literature survey the security and privacy in e-learning system is an important aspect to ensure the quality of e-learning service.

## II. Literature Review

Shaibu Adekunle Shonola and Mike Joy(2015) examined e-learning and m-learning systems and gave comparative analysis of possible security vulnerabilities and attacks. Client side systems should be secured from loss or theft. Learning content and assessment database on servers should

*March - April 2020*
*ISSN: 0193-4120 Page No. 10471 - 10478*

be protected from unauthorized access, modification or disclosure. Educational institutions are using access controls, firewalls, anti-virus and anti-malware software as protective measures. Heavy usage of mobile technology for unauthorized access to data degrades the network performance [2].

M. Durairaj and A. Manimaran(2015) discussed various types of attacks and security issues in cloud service delivery models of e-learning systems. This article has proposed a methodology to protect essential data from the attackers and make sure the availability of data to end user[3].

Adetoba B. T. et al. (2016) discussed recent developments in Personal Learning Environment, Biometric Authentication System and Security for Online Assessments[4]. Andrei Marius GABOR et al. (2017) proposed an algorithm to generate strong password to secure personal information from unauthorized access [5]. Bandara I.(2014) mentioned about the lack of adoption of IT policies and procedures while designing e-learning systems. Access to the right information at the right time is necessary.[6] Byeong Ho Kang, Hyejin Kim (2015) identified authentication as major security issue and introduced a framework for better authentication mechanism[7].

Defta (Ciobanu) Costinela – Luminitaa (2011) has evaluated security aspects of open-source elearning software Moodle. Study has suggested using encrypted SSL channels through web administration interface for transferring data between the system and administrators or content operators. Security features need to be integrated without affecting performance of the system[8]. Dragan Zlatkovic et al. (2019) has recommended specific international standards like ISO 27002 dealing with information security as design methodology for e-learning systems. This study claimed that PDCA is an appropriate methodology for module designing. Authors have pointed out that there are many non-compliant e-learning standards to be considered in information security which are flexible and adaptable[9]. Dr. M.U. Bokhari et al. discussed security requirements, possible attacks on the e-learning systems and counter measures to deal with these attacks. Study has focused on SSL, biometrics and basic cryptographic techniques as solution to the security threats[10].

Ekereke et al. 2019 reviewed security issues faced by e-learning platforms for Educational delivery in Nigeria. The paper has recommended remedies like digital watermarking, firewall, cryptographic techniques, SMS authentication and multi way biometric authentication [11]. Galina Akmayeva (2017) proposed Dynamic E-Learning Access Control and Copyright

Framework (DEACCF) which provide secured Access Control based on multi-factor authentication. It involves biometrics, digital signature, QR Code, password etc. Proposed framework claimed to improve user's security level and protect personal information and data within e-learning system[12].G. Sahaya Stalin Jose and C. Seldev Christopher(2018) discussed distributed data storage security for e-learning system. Authors have proposed use of data encryption standard to encode message and at the end save it on cloud. It leads to easy reconstruction and less time in Reed Solomon code. This method ensured easy and secured uploading and downloading of data in cloud based system[13].George SUCIU (2019) has focused on identifying and mitigating the risks of man-in-the-middle (MitM) attack when users connect to a Wi-Fi public network. Furthermore, they have evaluated several open source penetration testing tools which aid to the identification of vulnerabilities and propose proper security solutions for e-learning platforms in the context of using public Wi-Fi networks[14].

*March - April 2020*
*ISSN: 0193-4120 Page No. 10471 - 10478*

Osama A. Alsaadoun and Badar Al Lawati(2019) presented review of cyber security challenges that affect edutainment systems and gave practical recommendations to be considered by designers and operators of these systems. The blend of education, entertainment and technology is termed as Edutainment. Challenges identified are cyber bullying, privacy invasion, network intrusion and Ransomware. Authors have suggested a simplified IAM framework for edutainment security[15].

Mohammad Derawi(2014) has discussed several security aspects of e-learning platforms and examined significant concerns of open source learning system Moodle. The development requires that security services (e.g. authentication), encryption, access control, user management and their access rights to be implemented. The data transfer between the system and administrators or content operators should be implemented on encrypted SSL channels via the web administration interface. A secure learning platform must integrate all aspects of security and secure mechanism without affecting system performance[16].

Sakiba N (2016) tested the link between trust, privacy and security in the e-learning context. They focused on the threats of shifting to modern e-learning ecosystem like violation of confidentiality, integrity and availability in the asset assignment. Issues identified in E-learning systems are phishing attacks, identity theft, unauthorized access etc.[17] Ruth Raitman(2005) et al. also stated the importance of providing the sense of trust and privacy to make learner free in interacting and collaborating with others [18].

S. Farid et al. (2017) emphasized the need of privacy and personal identity of user in e-learning system. Authentication, authorization and non-availability of e-content in required time span considered as major threats in e-systems [19]. Taiwo Ayodele et al. (2011) proposed framework an Intelligent E-learning Preventive Mechanism (IEPM) which identify user's behavioral pattern to verify risk level and to suggest preventive actions[20]. Zuev V. (2012) provided the insights of security risks and vulnerabilities in e-learning environment. It has suggested the use of threat models in the planning of e-learning systems. This article focused on VLE surface attack [21].

Siti Salmah, Md Kassim et al. (2017) confirmed that availability, authentication and accountability are the most relevant trust factors using Multi-criteria Decision Making (MCDM) method through Analytical Hierarchical Process. This survey was conducted in Malaysian Higher Education institute[22]. N. Rjaibi and L.B.A Rabai(2018) proposed functional level security risk management model to quantify security level perception and the level of risk involved. Obtained values represent how stakeholders perceived security risks economically and predict how it will change over time to implement the security strategies[23].

## III. Adoption of E-learning in India

E-learning system provides a lot of opportunities for spreading out education and learning beyond the traditional classroom settings. Many educational institutions have adopted e-learning platforms due to its advantages in lower cost, faster delivery, effective teaching-learning process etc. Coursera, Khan Academy, NIIT, BIJU's, Unaacademy are some popular e-learning systems in India. These platforms provide various skill-based courses in IT, management, banking, finance, retail etc. With the advent of technology these courses are delivered through cloud courseware, cloud labs, interactive and collaborative learning platforms. Learners having smartphones, tablets, computers, laptops with internet connectivity could easily access these platforms. Corporate are using online training platforms internally for their employees. Some popular ones include Docebo, Absorb LMS, SAP Litmus, LearnUpon etc[24].

*March - April 2020*
*ISSN: 0193-4120 Page No. 10471 - 10478*

Many higher education institutions are using Moodle based e-learning environments to deliver and manage their courses. These customized learning management systems help in tracking student records. These systems provide facility of discussion forums to help students clarify their doubts. Teachers could share their reference reading material, question bank, question paper and to assess students remotely. It helps to provide customized feedback to individual student while keeping a digital record. Google classroom is a free collaboration tool for teachers and students. Teachers can create an online classroom, invite students, create and distribute assignments, track the student's progress, provide direct and real-time feedback etc. Offee model is a local content distribution platform. It is cloud based which deliver contents through mobile apps. Offee is an interactive learning and assessment tool. It enables sharing of study materials, mock tests, opinion polls, feedbacks and result analysis. Higher education institutes encourage use of learning through Massive Online Open courses(MooCs). They deliver skill based courses through internet, video libraries, DTH channels, virtual classrooms etc.

**IV. Security Issues in e-learning**

Processes, practices and technologies intended to protect computing systems and infrastructure from malicious and destructive activities carried out by unauthorized users are termed as cyber security. It covers communication networks, storage systems and user interfaces. A threat is something that may or may not happen, but has the potential to cause serious damage. Major security threats over internet are listed as follows (Rjaibi et al.[23]):

- Authentication – There should be uniquely identifiable entities in an information exchange, broken authentication leads to insecure communication.
- Availability – the state at which services are available for utilization as per permissions granted, not availability leads to denial of service.
- Confidentiality– privacy of information to the authorized user should be maintained from insecure object reference, information leakage and improper exception handling.
- Integrity– It verifies that information remains integral from unauthorized modification while in transit or storage. Problem would occur in case of cross site scripting, failure to confine URL access, injection flaws and malicious file execution.
- Intrusion detection- the ability to detect attempts to obtain unauthorized access

Cyber security was classified as:

- Disclosure: unauthorized access and release of proprietary and private information
- Deception: contaminating information to have incorrect representation or meaning
- Disruption: affecting the availability or quality of information and services
- Usurpation: malicious control of system components

In e-learning systems activities like online content delivery, assessment and submissions are more vulnerable to identity theft. Learners may copy the content through web or they may take help of others in completing their online submissions. Online systems are susceptible to security threats from software attacks like viruses, worms, macros, denial of service etc [9]. Learning resources, examination or assessment questions, students' results, user profile, forum contents, students' assignment and announcement are considered as asset in the e-learning system. Elearning systems are working either in a distributed network or over internet where multiple rights are associated with learner, instructors, content providers, administrators. Lots

of content and services are created, distributed, aggregated, disaggregated, stored, searched and used over these platforms. Digital Right Management (DRM) helps in protecting this content. In e-learning environment there is possibility of password misuse while attempting for online examinations, submitting assignments and downloading course materials. Password-based authentication systems are more vulnerable to phishing attacks. It requires proper user identification and verification techniques to be deployed [2, 9].

Cloud based online learning systems suffers threats like unauthorized access to data, data modification and destruction of data by intruders. It also suffers from network security, data integrity, data saggregation and data breaches at SaaS level. At PaaS level there would be issues in locating the data and privileged access. In IaaS level security threats are related to web service attack, SLA attack, distributed Denial of Service attack, Man in the Middle attack and DNS attack. E-learning platform of LinkedIn-Linda.com faced attack in December 2016 where student data around 9.5 million user accounts was hacked. Platforms like Lynda.com use centralized servers to store data. Even with the cloud it provides single attack points for data breach. Blockchain technology offers a significant solution to this problem. Blockchain is defined as "A decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks." As it maintains independent immutable copy which gets verified against all other records, there is no single point of attack possible. It leads to affordable and secured solution for protecting user's data.

## V. Security standards

Microsoft has developed the STRIDE model to help security engineers understand and classify the probable threats on a server. It consists of the six main types of threats spoofing, tampering, repudiation, information disclosure, denial of service and escalation of privileges. International Standardization Organization (ISO) has provided best practices for information security management through its set of ISO 27K standard [9]. Using this family of standards help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system[30]. An ISM is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying risk management process [31]. Identity and access management (IAM) is a suite of processes and all underlying technologies for the creation, management and usage of digital identities in a computing landscape. In practice, it covers the process of establishing the identity of users and governs the activities or services that users can perform or consume. IAM supports a range of security services including authentication, authorization, and activity auditing.

## VI. Security Counter Measures for E-learning systems

While developing e-learning safety methods internationally recognized standards needs to be considered. The system needs to implement security services such as authentication, encryption, access control, managing users and their permissions. E-learning system needs to be secured against manipulations from students and protect user's privacy. Authentication is vital in elearning to keep user's information secured. E-learning systems should implement authentication to assure the identity of the user he/she claims for. Biometric provides strong authentication as it cannot be stolen or duplicated easily though it

*March - April 2020*
*ISSN: 0193-4120 Page No. 10471 - 10478*

requires more investment. Counter measures suggested here includes access control through firewall, Digital Right Management on e-learning assets, digital watermarking, different cryptographic techniques and biometric authentication. Blockchain also helps in authenticating and securing the certification provided to learners by educators. Students will get full control on their online history records. Blockchain enables decentralization of education platforms by agreement than having a central authority. It offers peer-to-peer learning experience and solves the trust issues. LiveEdu e-learning platform is built using Ethereum blockchain. [26, 27, 30]

**VII. Conclusion:**

With increasing popularity e-learning systems required to be built standardized, secured, trusted and highly available to the user. Web based distributed nature of distance learning makes it vulnerable to security threats. Software attacks, deliberate espionage acts, cross site scripting, SQL injection, impersonation, identity theft are some common security issues in e-learning systems. Researchers have suggested use of various fusions of biometrics for user authentication, cryptographic techniques, appropriate authorization techniques and digital watermarking as counter measures. Security risk measurement standards should be adopted to quantify the security threats. Information security policies and procedures needs to be properly implemented to maintain quality of the system.

**References:**

[1] Latifa Ben Arfa Rabai, Neila Rjaibi, Anis Ben Aissa, “Quantifying security threats for Elearning systems”, IEEE Xplore: Nov 2012

[2] Shaibu Adekunle Shonola, Mike Joy, “Security issues in E-learning and M-learning Systems: A Comparative Analysis”, A Proceeding of 2nd WMG Doctoral Research and Innovation Conference (WMGRIC2015) 2015, Warwick UK, ResearchGate

[3] M. Durairaj, A. Manimaran, “A Study on Security Issues in Cloud based E-Learning”, Indian Journal of Science and Technology, Vol 8(8), 757–765, April 2015

[4] Adetoba B. T., Awodele O. , Kuyoro S. O. , “E-learning security issues and challenges: A review “, Journal of Scientific Research and Studies Vol. 3(5), pp. 96-100, May, 2016

[5] Andrei Marius GABOR, Marius Constantin POPESCU, Antoanela NAAJI, “Security Issues Related to E-Learning Education”, IJCSNS , VOL.17 No.1, January 2017

[6] Bandara I, Ioras F , Maher K., “Cyber Security Concerns in E-Learning Education.” In: Proceedings of ICERI2014 Conference, IATED, 0728-0734

[7] Byeong Ho Kang,Hyejin Kim,“Proposal: A Design of E-learning User Authentication System”, International Journal of Security and Its Applications Vol.9, No.1 pp.45-50, 2015

[8] Defta (Ciobanu) Costinela – Luminitaa, “Information security in E-learning Platforms”, Procedia Social and Behavioral Sciences 15, 2689–2693, 2011

[9] Dragan Zlatkovic , Nebojsa Denic , Milos Ilic , Milena Petrovic, “Security and Standardization at E-learning platforms”, ResearchGate, July 2019

[10] Dr. M.U. Bokhari, Dr. Salma Kuraishy, Sadaf Ahmad, "Security Concerns and Counter Measures in E-Learning Systems”, Conference Paper, ResearchGate, Nov 2010

[11] Ekereke, Layefa, Akpojaro, Jackson, “Security Challenges in Accessing E-Learning Systems: A Case-Study of Sagbama, Bayelsa State” , International Journal of Innovative Science and Research Technology, Volume 4, Issue 5, May 2019

*March - April 2020*
*ISSN: 0193-4120 Page No. 10471 - 10478*

[12] Galina Akmayeva, "Impact of Access Control and Copyright in E-Learning from User's Perspective in the United Kingdom", PhD thesis, Brunel University, London ,Dec 2017

[13] G. Sahaya Stalin Jose, C. Seldev Christopher, "Secure cloud data storage approach in elearning systems", Springer Science+Business Media, LLC, part of Springer Nature 2018 14.George SUCIU, Muneeb ANWAR, Cristiana ISTRATE,"Mobile Application and Wi-Fi Network Security for e-Learning Platforms", The 15th International Scientific Conference eLearning and Software for Education Bucharest, April 2019

[14] Osama A. Alsaadoun, Badar Al Lawati, "Realizing User Privacy and Security Issues in Edutainment e-Solutions", Springer Nature Switzerland AG 2019 X. Fang (Ed.): HCII, LNCS 11595, pp. 278–287, 277, 2019.

[15] Mohammad Derawi, "Securing E-learning Platforms", IEEE, 978-1-47995739/2/14,2014

[16] Nazmus Sakiba, "Security challenges for e-learning ecosystems", Master in Information Systems, Department of Computer Science, Norwegian University of Science and Technology, Jul-17

[17] Ruth Raitman , Leanne Ngo , Naomi Augar , Wanlei Zhou ,"Security in the Online Elearning Environment", Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05), 0-7695-2338-2/05 $20.00 © 2005

[18] S. Farid , M. Alam , G. Qaiser , A. A. U. Haq , J. Itmazi , "Security Threats and Measures in E-learning in Pakistan: A Review", Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 22 No. 3-2017

[19] Taiwo Ayodele , Charles A. Shoniregun, Galyna Akmayeva, "Towards E-Learning Security: A Machine Learning Approach", IEEE, 2011

[20] Zuev, V., "E-learning security models. Management", 7(2), 24-28,2012

[21] Siti Salmah Md Kassim, Mazleena Salleh, Anazida Zainal, Ab. Razak Che Husin, "Risk Tolerance and Trust Issues in Cloud-based E- Learning",ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing Article No.: 73 Pages 1–11, 2017

[22] N. Rjaibi, L.B.A Rabai, "How Stakeholders Perceived Security Risks? A New Predictive Functional Level Model and its Application to E-Learning",EAI Endorsed Transactions on Security and Safety, volume 5, Issue 15, e3, 2018

[23] Andrew Maas, Chris Heather, Chuong (Tom) Do, Relly Brandman, Daphne, Koller, Andrew Ng ,"MOOCs and Technology to Advance Learning and Learning Research", Offering Verified Credentials in Massive Open Online Courses", Ubiquity, an ACM publication, May 2014

[24] Romansky R., Noninska I. "Implementation of security and privacy principles in elearning architecture". In: Proceedings of the 29th International Conference on Information Technologies (InfoTech-2015), St. Constantine and Elena, Bulgaria (2015)

[25] Srivastava A. & Sinha S., "Information security through e-learning using VTE", 2013

[26] Sindhu Shivshankar, Dr.Sujni Paul, "E-learning environment – The security and privacy challenges focusing on the counter measures", International Conference on Developments of E-Systems Engineering, 978-1-5090-1861-1/15,2015 IEEE

[27] Neila Rjaibi, Latifa Ben, Arfa Rabai, Anis Ben Aissa, Mohamed Louadi, "Cyber

Security Measurement in Depth for E-learning Systems", IJARCSSE 2 (11), pp. 1-15, Nov- 2012
[28] https://www.classcentral.com/institution/moodle 22/12/2019
[29] https://support.udemy.com/hc/en-us/categories/204119748-Trust-Safety 24/12/2019
[30] https://in.pcmag.com/cloud-services/104247/the-best-online-learning-platforms-forbusiness29-12-19
[31] https://hackernoon.com/what-blockchain-technology-can-do-for-online-education88b6e2da7e7d
[32] https://www.iso27001security.com/html/27000.html
[33] https://www.iso.org/isoiec-27001-information-security.html