Lourdes Cecilia Ruiz Salvador
Óbuda University, Doctoral School on Safety and Security Sciences,
Ph.D. Candidate,
lourdes.ruiz@uni-obuda.hu

Carlos Lenin Alvarez Llerena
Doctoral School on Education, Hungary,
Ph.D. candidate,
caalvarezllerena@gmail.com

Dr. Huu Phuoc Dai Nguyen
Óbuda University, Doctoral School on Safety and Security Sciences
phuoc.daitt@bgk.uni-obuda.hu

DOI:

Research Paper

Received: October 26, 2021

Accepted: November 11, 2021

DIGITAL EDUCATION: SECURITY CHALLENGES AND BEST PRACTICES

Abstract: The COVID-19 pandemic and the rapid development of technologies have forced restructuring education at all levels. This change from traditional to digital learning demanded that teachers and students possess higher digital literacy. Moreover, it required them to be aware of the importance of security and its countermeasures to protect e-learning systems. The aim of this paper was twofold. First, it focused on security issues when using Moodle, Zoom. Blackboard, and edX. Furthermore, it offers best practices to address security threats and cyber-attacks from the outside network to e-learning systems. From this study, a cryptography mechanism arises as the best technique to protect the confidentiality, integrity, and authentication (CIA) of data on the e-platforms. However, it is not strong enough to mitigate cybersecurity attacks in e-learning systems. For that reason, it is suggested that the cryptography mechanism needs to be combined with other techniques such as biometric authentication, firewalls, IDS, digital watermarking, and security process models.

Keywords*: Digital education, security, challenges, countermeasures*

1. INTRODUCTION

Digital learning has been present in education for several decades. However, the rapid development of technologies and the COVID-19 outbreak shifted the education environment to home-schooling. Hence, the usage of technology at all education levels has become pervasive. For example, online learning platforms offer free courses to the public; video conferencing apps give students and instructors unlimited video time, translation, and collaborative editing capabilities. In addition, schools are partnering with television to broadcast educational content on separate channels(Li & Lalani, 2020). Technology can provide high quality and more flexible education experience without the restrictions posed in a traditional education environment, such as a strict schedule or a classroom. It can be an effective tool for joint, creative, and personalized learning. Technologies can integrate real-world problems into educational programs and offer teachers and students a wide array of feedback, reflection, and review opportunities. They can construct communities attracted to learning and generate new opportunities for teachers' professional development at local and global levels (National Academies of Sciences, 2018). Furthermore, corporations also use digital education to provide training to employees. Online education platforms offer various courses to improve business, safety, compliance, and technologies. Although technology provides several potentials within education, it also presents risks during implementation and deployment. Device manipulation, information leakage, network attack, and subsequent application platform effect are security threats found when using technology(Mawgoud et al., 2020; Serhan, 2020). Another aspect to be considered a barrier when using technology is the lack of knowledge regarding information security education(Olaza-Maguiña & De La Cruz-Ramirez, 2021). Consequently, this study focuses on these security threats and offers solutions that support teachers and students when applying technology for educational purposes.

2. SECURITY CHALLENGES

2.1 **Platform Security Issues**

2.1.1 Moodle (Modular Object-Oriented Dynamic Learning Environment)

Moodle is an open-source e-learning system. It uses PHP language and MySQL databases, offering various modules for teachers and students to create lessons, assignments, quizzes,

documents, and exercises. Furthermore, it helps teachers and learners communicate together through chat, surveys, or workshops. Brute force attack is a security vulnerability present in this platform. This attack guesses passwords and usernames by sending several demands to the webserver with a blank cookie field to reset the login failure count to zero. To think the username, many usernames are shipped with a random password. Usually, if the response from the server is extended, the chances of guessing the user are high. Another type of attack is a session hijacking attack. This attack takes control of a user session when successfully gaining or generating an authentication session ID. It is related to an attacker using captured, brute-forced, or reverse-engineered session IDs to take control of a legal user's Web application session while that session is still in progress. The session is handled in Moodle using two cookies: Moodle Session and Moodle Session Test, which can be interrupted because Moodle uses only SSL tunnels on the login service and a few administration services. This way, the HTTP requests are made in plaintext, which may be intercepted and decoded. An attacker can use this data in its HTTP request to control the target user session. Likewise, several types of attacks are related to authentication, availability, confidentiality, and data integrity in the Moodle system (Kumar & Dutta, 2011).

2.1.2 Zoom

Zoom is a platform that helps students or teachers to communicate remotely. It brings many advantages, such as easy installation, a friendly interface, and free usage. However, it faces several security threats such as zoom bombing, end-to-end encryption, Mac spying, windows remote code execution, Cisco Talos vulnerabilities (Matt Miller, 2020). In 2021, (Charlie Osborne, 2021) reported three-bug attack chains used remote code execution (RCE) on a victim's machine. Another research (Paul Wagenseil, 2021) identified more than ten types of security and privacy issues in Zoom. According to (Ahmed 2020), many security holes in Zoom were recognized, and two of them can let hackers read and steal users' data.

2.1.3 Blackboard

Blackboard is a comprehensive digital learning space to increase users' personalized learning at any time and anywhere. It offers many tools to support learning and teaching activities such as Blackboard Analytics, Grade center, blackboard assessment, accreditation, blackboard

engagement, and more. Nevertheless, it is also vulnerable to many security issues like the other platforms (Philip, 2020). For instance, in 2010, 84 security issues related to the Blackboard platform were encountered. Notably, the LaQuSo team reported three significant types of attacks in the SP5 version of blackboards like cross-site request forgery, cross-site scripting attacks, and authorization vulnerabilities (M. V. Eekelen et al., 2013).

2.1.4 edX Platform

This platform provides a high-quality learning experience to various universities, organizations, and institutions. It introduces the edX data package, which includes collecting usage data from courses on the course pages (edX, 2021). However, it presents several vulnerabilities for users, such as cross-site scripting (XSS), password phishing, server-side code execution, and RDX data identification (Lynch & Friis, 2018).

- *XSS:* It is one of the most popular security issues on the Internet. It creates a chance for hackers to inject client-side scripts into the site. The XSS worm was designed to inject every section, subsection, or unit for every course and put it in the module. Moreover, this worm can automatically use malicious scripts to infect every unit on the course.
- *Password phishing:* Phishing attacks are more dangerous to students who share a password between various sites, and hackers may access students' accounts within the edX platform.
- *RDX Data Identification:* RDX is another way of security and functionally tradeoff. It can produce valuable tools to search student retention rates and factors that support learners and efficiently use the site resources. It also increases the effectiveness of online education. However, it provides large datasets to outside researchers, potentially risky.

2.2 **External Cyber Attacks**

2.2.1 Malicious Attacks

Computer viruses, malware, Trojan are malicious programs that may change or damage the operating system without the user's permission, using attached files in the e-mail or advertisements (Huu Phuoc Dai et al., 2016). When students or instructors download the resources in an e-system, it is easy to download malicious codes simultaneously. Furthermore, students can use their own devices to find information, cooperate, or communicate with other

students for learning on and off-campus. Consequently, it is more difficult for the data controller to ensure the security of the network system against viruses, Trojans, or malware (Bandara et al., n.d.). Additionally, students are the primary users of social media networks. Therefore, this can create a suitable environment for spreading viruses, malware, and other viruses via these social media websites.

2.2.2 Availability attack

This attack aims to interrupt the connectivity resources or limit the bandwidth of the E-Systems. Moreover, it also tries to gain privileged access to the information or services in the learning platform. DoS or DDoS attacks are not new types of threats. However, their damage is much more dangerous than in previous years (Kaspersky, 2021). The volume of DDoS attacks and their complication has dramatically increased due to the decreasing price of launching this type of attack. Therefore, it is tough to detect and protect the systems against them. According to the Kaspersky report, there were a significant number of DoS attacks in e-learning systems from 2019 and 2020 (Securelist, 2020). It increased 550% in 2020 compared to 2019 at the same time (January). Zoom is the most popular platform under attack, and Moodle is the second one. Moreover, adware, downloaders, and Trojans were encountered in nearly 99% of total registered infection attempts.

2.2.3 Confidentiality attack

This attack does not mainly focus on changing data content but limit data access and distribution activities (Kumar & Dutta, 2011). This attack has three major categories: insecure cryptographic storage, insecure direct object reference, information leakage, and improper error handling(Stapić et al., 2008).

- *Insecure cryptographic storage:* e-learning systems rarely use cryptographic mechanisms to protect data. Therefore, sensitive data can be kept in storage or a database without encryption.
- *Insecure direct object reference:* e-system uses object references (files, data records, and primary keys) in the web interfaces but without using any methods of authorization checks

- *Information leakage and improper error handling:* sensitive information or data can be revealed unintentionally via error messages.

2.2.4 Integrity attacks

There are many types of vulnerabilities for e-learning from external attacks such as malicious codes such as CSS or XSS, cross-site request forgery (CSRF), direct SQL code injection in the web pages, Buffer overflow, failure to restrict URL access, Injection flaws, and malicious file execution(Costinela-Luminiţa & Nicoleta-Magdalena, 2012)(Rjaibi et al., 2012)(Stapić et al., 2008).

- *Cross-site scripting (CSS) or XSS:* malicious code injection attacks mainly target websites and display user content without checking and encoding the information entered by users dynamically.
- *Cross-site request forgery (CSRF):* a dangerous vulnerability because it can execute an unauthorized action in the platform with legal user access and consent.
- *Buffer overflow (Buff):* Using code to attempt to store data in a possible buffer without validating its size (Rjaibi et al., 2012)
- *Fail in restriction URL access (FURL*): the attackers can take advantage of the limitation of a small subset of privileged users into some system resources to target some operations (Kumar & Dutta, 2011).
- *Injection flaws (InjecF):* hackers can inject the input data (SQL query) in the client workstation into the application to read, modify, or execute sensitive data on the database (Kumar & Dutta, 2011).
- *Malicious file execution:* malicious codes can be integrated during the upload function, and the system cannot manage the performance of uploaded files.

2.2.5 Authentication attacks

This kind of attack happens when hackers illegally gain users' passwords and try to have free access to the materials on the e-learning systems (Stapić et al., 2008). In addition, when this attack occurs, it is easy for hackers to have a chance to perform other types of attacks, for example, availability, confidentiality, and integrity attacks. There are two major categories:

broken authentication and session management and insecure communication attacks (Rjaibi et al., 2012)(Stapić et al., 2008).

- *Broken authentication and session management:* Hackers can capture or steal legal users' authenticated sessions, including active sessions, passwords, and session tokens.
- *Insecure communication:* During data transmission, session tokens or sensitive information without using an encryption mechanism can be taken by attackers to access unprotected conversations and take a user's credentials.

3. COUNTERMEASURES

Different countermeasures to protect e-learning systems are described in this section:

3.1 Cryptography

Cryptography is a technique to guarantee data confidentiality and non-disclosure to unauthorized parties (Fayziyeva et al., 2019)(Costinela-Luminita, 2011). It is a process to convert data from origin to unintelligible format. It can be used in many electronic systems with various tools to ensure data transmission on the Internet. The cryptography mechanism uses many mathematical algorithms related to information security to protect data, such as confidentiality, integrity, and authentication. Symmetric key encryption and asymmetric key encryption are crucial types of encryption methods.

3.2 Digital Right Management

Laws, beliefs, and practices define digital rights. In the virtual space, digital right management (DRM) is an important strategy to be integrated, especially in e-learning, to diminish the risks related to e-learning assets, services, and resources (El-Sofany et al., 2013). It constitutes an application for e-education with standards, technologies to support the sharing or reuse of e-learning resources.

3.3 Distributed Firewall solution

Distributed firewalls include many security software applications in host-resident to protect organizations' networks, users, and servers against unexpected intrusion (Fayziyeva et al., 2019).

However, there is a significant difference between a personal firewall and distributed firewall. The latter gives more benefits such as central management, logging reports, and access control granularity. These features can be used in enterprises to cooperate with security policies inside the firewall. Besides, a firewall offers various benefits, such as protecting the networks or systems against internal and external attacks, diminishing single points of failure, securing remote end-user machines, and safeguarding hosts.

3.4 Biometric authentication

Traditional techniques for authentication like passwords, smart cards, digital signatures, and digital certificates are used to keep passwords secret. In parallel, biometric authentication is a new method to increase security. It is also the best choice to help users avoid password misusage when submitting assignments and papers and downloading course materials (Fenu et al., 2018)(Adetoba B. T., 2016).

3.5 Digital watermarking

Digital watermarking is a new method that allows users to put hidden copyright notes, audio, videos, image signals. Therefore, unauthorized usage in e-learning systems can be prevented by using digital watermarking (Edgar R. Weippl, 2005). There are two major types of digital watermarking, visible and invisible watermarking (Neena et al., 2016). The former uses embedded algorithms, less complex computation, and easy recognition. The latter makes it hard for viewers or readers to see or identify watermarking.

3.6 Countermeasures against cyber attacks

Due to the Internet-based environment, the e-system also faces cyber-attacks as the Internet. Therefore, according to (Huu Phuoc Dai et al., 2016)(Stapić et al., 2008), there are many ways to protect e-learning against the cyber-attacks, such as using secure protocol HTTPS, instruction detection system, firewalls, and cryptography mechanisms. These methods can ensure the integrity, availability, authentication, and confidentiality of digital systems against external attacks. Moreover, there exist a variety of solutions to secure e-learning systems. Notably, for Moodle, log in with captcha and SSL are best practices to avoid brute force attacks and secure the session between a web server and a browser (Kumar & Dutta, 2011). Furthermore, applying a

biometric multi-function to authenticate students in e-learning platforms, including face, voice, touch, mouse, and keystroke, is a potential, flexible, and reliable solution to identify students (Fenu et al., 2018). E-learning is a cloud-based environment. It takes advantage of cloud computing technologies. However, several security issues related to cloud computing can be present. Hence, various mechanisms can be used to address these security issues, such as SMS information security, biometric information security, token-based information security, access control list, digital signature information security, cryptography, and secure e-learning platform based on SOA-based architecture (El-Sofany et al., 2013). A promising method released in several universities in the USA and Europe is Blockchain (based on mathematics and cryptography) to protect or prove documents in e-learning systems from fraud or security problems (Natalya et al., 2018). This method dramatically changes education because it can help create a complete system for managing educational achievements. In addition, to exercise a proactive approach against cyber-threats in e-learning systems, a security management model for e-learning systems should be deployed. It includes a cycle with four stages: Plan, Implements, Evaluate, and Maintain. This process can help the system predict the threats and warn data users of emerging and evolving threats or risks. It presents several special conditions for the input to comply with the Data Protection Act. Besides, in this model, there is a comprehensive combination between staff and users by applying a well-administered plan in the organization to mitigate cybersecurity threats

4. CONCLUSIONS

Education had to adapt to the pandemic situation quickly. Traditional learning methods were shifted to digital learning in formal educational institutions and corporate training. There is a wide variety of tools for digital learning. However, students and teachers must possess digital literacy to face this new era in education. As for the capabilities needed in e-learning tools, these tools must provide an equal learning opportunity for all the students. Including individuals with disabilities, people in developing countries with unreliable internet connections and electronic devices are scarce. E-learning has become prevalent in many countries over the world due to the COVID-19 outbreak. Therefore, the security of several e-learning platforms is a significant concern. This paper indicates the security issues related to some e-platforms for learning such as

Moodle, Zoom, Blackboard, and edX. Besides, many types of cyber-attacks from the outside network to e-learning systems are also described. It also provides best practices to address security threats and cyber-attacks towards e-education systems. Remarkably, a cryptography mechanism is the best technique to protect the confidentiality, integrity, and authentication (CIA) of data on the e-platforms. However, it can be seen that one method is not strong enough to counter the whole system. As a consequence, it needs to combine different methods like biometric authentication, firewalls, IDS, digital watermarking, and security process models with various levels of security standards to manage and control data processes in e-learning systems to mitigate cybersecurity problems and cyber-attacks

ACKNOWLEDGEMENT

This article is supported by the national grant "2020-1.1.2-PIACI-KFI-2020-00099" on the project "Learning Profile Based, Digital skills development methodologies and development of educational teaching tools in applications," Óbuda University, Budapest, Hungary.

REFERENCES

Adetoba B. T., A. O. and K. S. O. (2016). E-learning Security Issues and Challenges: A Review. *Journal of Scientific Research and Studies*, *3*(5), 96–100.

Ahmed, R. (2020). *Zoom Vulnerabilities Demonstrated in DEF CON Talk*.

Bandara, I., Ioras, F., & Maher, K. (n.d.). *CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION*.

Charlie Osborne. (2021). *Critical Zoom vulnerability triggers remote code execution without user input*.

Costinela-Luminiţa, C. (Defta), & Nicoleta-Magdalena, C. (Iacob). (2012). E-learning Security Vulnerabilities. *Procedia - Social and Behavioral Sciences*, *46*, 2297–2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Costinela-Luminita, D. (2011). Information security in E-learning Platforms. *Procedia - Social and Behavioral Sciences*, *15*, 2689–2693. https://doi.org/10.1016/j.sbspro.2011.04.171

Edgar R. Weippl. (2005). E-LEARNING. *ADVANCES IN INFORMATION SECURITY*, *16*.
edX. (2021). *Documentation for edx.org and the OpenedX Community*.
El-Sofany, H. F., Tayeb, A. Al, Alghatani, K., & El-Seoud, S. A. (2013). The impact of cloud computing technologies in E-learning. *International Journal of Emerging Technologies in Learning*, *8*(SPL.ISSUE), 37–43. https://doi.org/10.3991/ijet.v8iS1.2344
Fayziyeva, D. S., Yuldasheva, N. S., & Ugli, I. S. Z. (2019). Security issues in E-Learning system. *International Conference on Information Science and Communications Technologies: Applications, Trends, and Opportunities, ICISCT 2019*, *April*. https://doi.org/10.1109/ICISCT47635.2019.9011971
Fenu, G., Marras, M., & Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, *113*, 83–92. https://doi.org/10.1016/j.patrec.2017.03.027
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
Kaspersky. (2021). *DDoS Protection*.
Kumar, S., & Dutta, K. (2011). Investigation on security in LMS moodle. *International Journal of Information Technology …*, *4*(1), 233–238.
Li, C., & Lalani, F. (2020, April 29). *The rise of online learning during the COVID-19 pandemic*. World Economic Forum. https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/
Lynch, A., & Friis, E. (2018). *Security Analysis of the edX Platform The edX Platform*.
M. V. Eekelen, R. Moussa, Engelbert Hubbers, & Roel Verdult. (2013). Blackboard Security Assessment. *CTIT Technical Report Series*, *April*.
Matt Miller. (2020). *Zoom security issues*.
Mawgoud, A. A., Taha, M. H. N., & Khalifa, N. E. M. (2020). Security Threats of Social Internet of Things in the Higher Education Environment. *Studies in Computational Intelligence*, *846*, 151–171. https://doi.org/10.1007/978-3-030-24513-9_9
Natalya, M., Alexey, K., & Alexander, L. (2018). *Analysis of E-learning in Digital Economy*. *January 2018*. https://doi.org/10.2991/emle-18.2018.167

National Academies of Sciences, E., and M. (2018). How people learn II: Learners, contexts, and cultures. In *How People Learn II: Learners, Contexts, and Cultures*. National Academies Press. https://doi.org/10.17226/24783

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

Olaza-Maguiña, A. F., & De La Cruz-Ramirez, Y. M. (2021). *Digital Education and Information Security in Obstetric Students in COVID-19 Pandemic Times in Peru*. 97–107. https://doi.org/10.1007/978-3-030-85893-3_7

Paul Wagenseil. (2021). *Zoom security issues: Here's everything that's gone wrong (so far)*.

Philip, A. (2020). *Information Security Reading Room The Legal System and Ethics*.

Rjaibi, N., Rabai, L., Aissa, A., & Louadi, M. (2012). Cyber Security Measurement in Depth for E-learning Systems. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(11), 1–15.

Securelist. (2020). *Digital Education: The cyber risks of the online classroom*.

Serhan, D. (2020). Transitioning from Face-to-Face to Remote Learning: Students' Attitudes and Perceptions of using Zoom during COVID-19 pandemic. *International Journal of Technology in Education and Science*, *4*(4), 335–342. https://doi.org/10.46328/IJTES.V4I4.148

Stapić, Z., Orehovački, T., & Danić, M. (2008). Determination of optimal security settings for LMS Moodle. *MIPRO 2008 - 31st International Convention Proceedings: Digital Economy - 5th ALADIN, Information Systems Security, Business Intelligence Systems, Local Government and Student Papers*, *5*, 84–89.