ISSN 2347 - 3983
Volume 9. No.12, December 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter089122021.pdf
https://doi.org/10.30534/ijeter/2021/089122021

Implicated Factors in the Success of E-learning Platforms and Online Laboratories of Experimenting along with Enhancement of their Cybersecurity

Yassine Larbaoui[1], Ahmed Naddami[2], Ahmed Fahli[3]
[1]Electrical engineering department, University Hassan 1er, Morocco, Yassine.larbaoui.uh1@gmail.com
[2] University Hassan II, National High School for Electricity and mechanics, Casablanca, ahmed.naddami@gmail.com
[3] Electrical engineering department, University Hassan 1er, Morocco, fahli@uhp.ac.ma

Received Date : November 08, 2021 Accepted Date : November 29, 2021 Published Date : December 07, 2021

ABSTRACT
This paper presents implicated factors in the success of e-learning platforms and online laboratories of experimenting from two different aspects of view: technical engineering aspect and scientific research aspect. These presented factors are categorized according to different levels: educational level, pedagogical level, technological level, service providing, marketing and management. Furthermore, this paper presents how to enhance the cybersecurity of e-learning platforms and online laboratories of experimenting whereas defining the technical characteristics and financial criteria to choose hardware and software products to concretize this cybersecurity.

Key words: E-learning, education, cybersecurity, pedagogy, online experimenting, online laboratory, success factors.

1. INTRODUCTION

Pedagogies of education [1] are consistently evolving by exploiting the technological evolutions of computers and other electronic devices that rely on the use of internet and networking protocols implicated in telecommunication fields. This evolvement [2], [3] is significantly contributing in traditional education and enabling to structure distance education while reaching numerous categories of scattered populations around the world.

Nevertheless, pedagogical aspects of distance education are still under-evolved comparing to the evolvements of actual technologies that support e-learning, virtual experimenting and remote experimenting.

This under-evolvement is mostly due to the high pace of technological evolutions, where engineers and researchers condense their focus on the development of exploitable resources in education more than focusing on advancing traditional tools of pedagogy, because these resources may simply be utilized during classic courses or be used as complementary resources to them.

Pedagogies of education serve many aspects to the benefit of students, such as socializing, learning communication skills, expressing opinions and ideas, apprehending various knowledge, experimenting in practical fields of science and technologies, etc. However, many technologies of distance education and online experimenting cannot stand alone to serve a great part of these aspects, because they need to be cooperated.

The exponential advancement of e-learning technologies in our nowadays is globally recognized, while diversities of these technologies are being integrated by many educational establishments around the world during the global pandemic of COVID-19 [4], [5]. There have been intercontinental efforts to support educational courses and pedagogical services without obligating students, teachers and staff of educational establishments to leave their homes [6]. These efforts have been encountering many challenges, technically and pedagogically, while giving birth to plenty opportunities [7].

There are many published research papers present advantages, disadvantages and success factors of e-learning [8], [9], [10], whereas other papers compare between online laboratories [11], [12], [13]. However, the majority of these papers treat e-learning and online laboratories from general aspects of view [14], and do not analyze them from the technical engineering aspect of development, deployment, maintenance, maintaining, extending and optimizing.

As an example on relevant research projects, the published papers [15], [16], which treat the availability, reliability, flexibility and quality of e-learning without gritting deeper into the technical engineering factors that have an influence on e-learning platforms. There are other relevant papers, which treat the cybersecurity of remote labs [17] and flexibility of remote experiments [18].

This paper is distinguished by presenting the implicated factors in the success of e-learning platforms and online laboratories of experimenting at the levels of education, pedagogy, service providing, technology, marketing and management. In addition, this paper is treating these implicated factors from two different aspects of view:

technical engineering aspect and scientific research aspect. Furthermore, this paper presents how to establish an enhanced cybersecurity on e-learning platforms and online laboratories whereas presenting the technical characteristics and financial criteria to choose hardware and software products that concretize this cybersecurity.

This paper is structured as follow: Section 2 presents implicated factors in the success of e-learning platforms. Section 3 presents implicated factors in the success of online laboratories of experimenting. Section 4 presents how to reinforce the cybersecurity of online laboratories and e-learning platforms along with technical characteristics and financial criteria to choose hardware and software products in order to concretize this cybersecurity. Finally, section 5 for conclusion.

2. IMPLICATED FACTORS IN THE SUCCESS OF E-LEARNING PLATFORMS

There are many aspects to consider in order deploying successful platforms of e-learning. These aspects can be categorized according to different levels such as educational level, pedagogical level, technological level, service providing, marketing and management. Therefore, in this section we present the most important factors to deploy successful e-learning platforms.

2.1 Success Factors of E-learning Platforms at the Educational Level

This subsection presents relevant factors to deploy successful e-learning platforms at the educational level, which are as follow:

1. Providing different courses for different educational levels.
2. Supporting theoretical contents of courses using document, PDFs, PowerPoints, Videos, etc.
3. Supporting online classes using video conferencing.
4. Supporting textual communication between teachers and students during online classes using chat boxes.
5. Supporting online collaboration between students using educational forums categorized according to course topics and subjects.
6. Supporting supplementary course sessions.
7. Supporting the saving of generated videos during video conferences of course sessions, in order to be accessed by students after the conduction of these sessions.
8. Providing training certificates in educational topics and in professional fields, such as software development, networks administration, cybersecurity, etc.

2.2 Success Factors of E-learning Platforms at the Pedagogical Level

This subsection presents relevant factors to deploy successful e-learning platforms at the pedagogical level, which are as follow:

1. Supporting interactive face-to-face contact between professors and students using real-time video conferencing during class sessions, in order to have an interactive human contact.
2. Supporting real-time quizzes, to quiz students about their cumulated knowledge after course sessions.
3. Supporting real-time exams, to conduct necessary exams for each class.
4. Supporting online experiments, to provide the practical aspect of educational pedagogies.
5. Providing online tools for attachment files of reports, forms of non-real time quizzes and documents of non-real time exams, in order to be assessed by professors.
6. Providing online service for courses scheduling, in order to determine scheduling characteristics for each course: start-date, end-date, participants, etc.
7. Integrating an online service dedicated to provide grades to students.
8. Providing forums for general topics of collaboration between students
9. Providing an online service for educational social media, in order to support news defusing and communication between, students, professors, lecturers and staff of educational establishment.
10. Providing tutorials to students on how to use the services of deployed platform for e-learning.
11. Supporting the creation and programs of online clubs, in order to implicate students in diversified activities.
12. Providing training certificates in educational topics and in professional fields, such as software development, networks administration, cybersecurity, etc.

2.3 Success Factors of E-learning Platforms at the Level of Service Providing

This subsection presents relevant factors to deploy successful e-learning platforms at the level of service providing, which are as follow:

1. Ensuring the reliability of deployed platform for e-learning and its integrated services for 24 hours, seven days a week.
2. Deploying technologies that provide sufficient binary data throughputs in Mbps (Megabits per second), in order to support the expected volumes of TCP/IP (Transmission Control Protocol/Internet Protocol) packets.
3. Integrating an identification service where the identity of each student, professor and employee is verified by using emails and passwords.
4. Integrating authentication utilities to verify access credentials of students, professors, lecturers and instructors before allowing any of them to access courses and online classes.
5. Integrating flexible scheduling services for online classes.
6. Reinforcing the cybersecurity of deployed platform for e-learning [17], deployed networks and deployed

resources, in order to reinforce the reliability of deployed services and protect credentials of professors, employees and students.
7. Integrating online functionalities to forward news and relevant information to the emails of students, professors, employees and other apparatus of interest in the form of newsletters and alarming messages.
8. Improving online services to be accessible on web-browsers, computers, cellphones, IPads, etc.
9. Providing offline services of e-learning at the local level of educational establishment [19], where students, professors and staff may access the deployed services of e-learning without using internet as long as they are at the geographical boundaries of their educational establishment.
10. Integrating online services for questioning and complaining.
11. Training professors and employees to use their concerned services on deployed e-learning platform.

2.4 Success Factors of E-learning Platforms at the Technological Level

This subsection presents relevant factors to deploy successful e-learning platforms at the technological level, which are as follow:

1. Relying on versatile digital resources for theoretical contents of courses that can be accessed on the majority of devices (computers, phones, Tablets, IPads, etc.).
2. Relying on technologies of real-time video conferencing that can be supported on web-browsers or software applications without complications generated by software technicalities on devices.
3. Developing software applications dedicated for the online services of educational establishment.
4. Using supplementary power supply resources to be used when encountering technical problems at public networks of power supply.
5. Deploying firewalls, networking roles, Intrusion Prevention Systems (IPSs), Detection Prevention Systems (IDSs), Virtual Private Networks (VPNs) and other technologies of hardware and software to reinforce the cybersecurity of locale networks and online services [17].
6. Providing online environments for virtual experiments and simulation-based experiments.
7. Providing online environments for remote experiments.
8. Deploying automated answering services (such as by deploying automated chatting services relying on chat-bots) for repeated questions and redundant patterns of complains.

2.5 Success Factors of E-learning Platforms at the Levels of Marketing and Management

This subsection presents relevant factors to deploy successful e-learning platforms at the levels of marketing and management, which are as follow:

1. Deploying user-friendly services and attractive web designs.
2. Creating web pages on social Medias, such as Facebook (Meta), Instagram and Twitter, in order to advertise the provided services on the e-learning platform.
3. Creating advertising campaigns on internet periodically, such as by defusing advertising videos on YouTube, Google Ads and Facebook (Meta) Ads.
4. Creating video channel on You Tube to share events, news, video examples of online courses, etc.
5. Relying on advertising posters periodically.
6. Creating web pages on the e-learning platform listing the competences and academic credibility of professors and staff.
7. Creating web pages on the e-learning platform to advertise accomplishments of students in terms of excellent grades, conducted projects and awards.
8. Coordinating collaborations with enterprises and institutions in order to provide professional certificates to students.
9. Coordinating collaborations with different universities around the world, in order to provide double-diplomats to students.
10. Using Customer Management Systems, Enterprise Resource Planning software (ERP) and Content Management Systems to handle data of classes, professors, students and staff, such as by using SAGE (50 Cloud ciel) and KONOSYS.

3. IMPLICATED FACTORS IN THE SUCCESS OF ONLINE LABORATORIES

There are different types of online laboratories (virtual labs, remote labs and simulation-based laboratories), which differentiate from each other in terms of used resources and provided approximations to real experiments in hands-on laboratories, whereas the success of e-learning platforms is relatively related to the integration of these online laboratories. Therefore, we dedicate this section to present relevant factors to deploy successful environments of online experimenting.

3.1 Success Factors of Online Laboratories at the Pedagogical Level

This subsection presents success factors of online environments of experimenting at the pedagogical level, which are as follow:

1. Providing scheduling services for each deployed experiment, in order to coordinate between these experiments and their corresponding courses.
2. Providing online utilities for identification and

authentication, to control the access to each online experiment.
3. Integrating online environments for collaborative experiments, where students may share one online experiment where there is one conductor at a time while others observing.
4. Cooperating online utilities of face-to-face contact between participants during collaborative online experiments by relying on real-time video conferencing.
5. Cooperating online utilities for textual communication and data defusing between participants during collaborative online experiments.
6. Supporting real-time online quizzes on conducted online experiments.
7. Providing utilities to submit reports on conducted experiments, in order to be assessed by professors.
8. Providing high approximations to physical resources used in hands-on laboratories in terms of shapes of instruments, functionalities and manipulation such as by using VISIR system [20], [21].
9. Providing digital documents to students in order to structure the conduction of online experiments according to the requirements of their corresponding courses.

3.2 Success Factors of Online Laboratories at the Educational Level

This subsection presents success factors of online environments of experimenting at the educational level, which are as follow:

1. Providing digital resources to support theoretical contents of online experiments.
2. Providing online utilities to compare theoretical results and practical results of online experiments.
3. Providing online tools for measurements in electronics, electricity and other educational fields of experimenting.
4. Providing tutorials to students showing them how to exploit these online experiments.

3.3 Success Factors of Online Laboratories at the Level of Service Providing

This subsection presents success factors of online environments of experimenting at the level of service providing, which are as follow:

1. Ensuring the availability and reliability of online experiments for 24 hours, 7 days a week.
2. Deploying necessary hardware of network to provide sufficient binary data throughputs in Mbps, in order to support expected numbers of online experimenting sessions.
3. Providing open services of online experimenting for enrolled students with less restriction in terms of scheduling and authentication.
4. Integrating online services dedicated to the questions and requests of students in the concerns of online experiments.
5. Reinforcing the cybersecurity of deployed resources for online experimenting [17], in order to solidify the availability and reliability of their resources whereas protecting the credentials of online experimenters.

3.4 Success Factors of Online Laboratories at the Technological Level

This subsection presents success factors of online environments of experimenting at the technological level, which are as follow:

1. Providing web-user interfaces for online experiments that can be used on different web-browsers.
2. Providing software applications for online experiments that can be used on different devices.
3. Using cross-platform programming languages to develop web-user interfaces and client module applications for online experiments, in order to avoid complications dependent on software environments of used devices by students for online experimenting.
4. Cooperating various environments of online laboratories into the same environment of online experimenting, in order to implicate virtual experiments, remote experiments and simulation-based experiments.
5. Deploying online environments of remote experimenting where the possibility of interconnecting between the instruments and hardware components of deployed experimenting plants according to different combinations.
6. Relying on Time Division Techniques (TDM), in order to share the exploit of the same hardware of an experiment between multiusers simultaneously or nearly simultaneously [22], [23], [24].
7. Relying on Software Multiplexing Techniques in order to experiment on a remoted hardware according to different combinations between components and instruments while being exploited by multiusers nearly simultaneously [24]. As an example, having two web-user interfaces for two different remote experiments that exploit the same hardware according to two different combinations.
8. Using Virtual Local Area Networks (VLANs) to separate the hardware and software resources of online experiments from other networks that may be accessed by staff, professors and students, in order to avoid potential cyberattacks that rely on Social Engineering.
9. Relying on IPS, IDS, Firewalls, VPNs, Antiviruses and networking roles dedicated to secure the hardware and software of online experiments at the local level of educational establishment and through the internet [17].

Table 1: Providers and hardware products for cybersecurity.

IPS Hardware	IDS Hardware	Firewall Hardware
Trend Micro.	Cisco Systems Inc.	Bitdefender BOX.
Darktrace.	Internet Security Systems Inc.	Cisco (such as ASA 5500-X).
Cisco Systems Inc.	Intrusion.com Inc.	CUJO AI Smart Internet Security Firewall.
NSFocus.	Symantec Corp.	Fortinet FortiGate (such as 6000F Series).
FortiGuard IPS.	PGP Security.	Netgear ProSAFE.
		Palo Alto Networks (such as PA-7000 Series).
		Netgate pfSense Security Gateway.
		SonicWall Network Security Firewalls.
		Sophos XG Firewall.
		WatchGuard Firebox (such as T35 and T55).

Table 2: Software products for cybersecurity.

IPS Software	IDS Software	Firewall Software and Antivirus
SolarWinds Security Event Manager.	SolarWinds Security Event Manager.	Bitdefender Total Security.
Datadog Real-time Threat Monitoring.	Bro.	Avast Premium Security.
Splunk.	OSSEC.	Norton 360 Premium.
Sagan.	Snort.	Panda Dome Essential.
OSSEC.	Suricata.	Webroot AntiVirus.
Open WIPS-NG.	Security Onion.	ZoneAlarm.
Fail2Ban.	Open WIPS-NG.	GlassWire.
Zeek.	Sagan.	Comodo Firewall.
	McAfee Network Security Platform.	TinyWall.
	Palo Alto Networks.	Windows Defender.

10. Adapting the hardware and software of hands-on laboratories to be accessed and exploited through internet [24].
11. Sharing hardware resources between educational establishments and institutions [25].
12. Deploying environments of remote experiments where the possibility of building circuits of electronics and electricity from scratch, whereas opening the way to conduct different remote measurements on them.
13. Deploying scalable environments of online laboratories where the possibility to add new resources of hardware and software for online experimenting [26], [27].

3.5 Success Factors of Online Laboratories at the Levels of Marketing and Management

Implicated factors in the success of online laboratories at the levels of marketing and management are various, such as publicity on social media, advertising campaigns using posters, creating channels on YouTube to publish advertising tutorials, collaborating with universities and institutions, etc. In general, we may say that these factors are similar to the ones implicated in the success of e-learning platforms at the levels of marketing and management, which are listed in Section 2. Nevertheless, we may list additional factors, such as providing online demos with open access to encourage institutions and universities to collaborate with these online laboratories and attract more attention and more financial support (or even attract grants).

4. TECHNOLOGY CHOICES TO ESTABLISH THE CYBERSECURITY OF E-LEARNING PLATFORMS AND ONLINE LABORATORIES

There are many measures to be conducted in order to establish the cybersecurity of networks that deploy e-learning platforms and online experiments such as by deploying Firewalls, Intrusion Prevention Systems (IPSs), Intrusion Detection Systems (IDSs), Virtual Private Networks (VPNs) and Antiviruses. In addition, there are many technical standards known at the global scale to secure networks and web-services, such as ISO/IEC 27033 [28] and standards of RIT (Rochester Institute of Technologies) [29], which we can rely on to deploy the cybersecurity of e-learning platforms and online laboratories of experimenting.

As an example of conducted research projects on the cybersecurity of e-learning and online laboratories, paper [16] presents measures to deploy secure web services of e-learning and remote experimenting on remote laboratories, whereas proposing countermeasures against potential cyberattacks of

Table 3: Technical characteristics and financial criteria to choose hardware products for cybersecurity.

Criteria	Description
Price of hardware	Choosing the appropriate price depending on the financial aspect of investment.
Price of hardware maintenance	Price of hardware maintenance after expiring the guarantee may discourage buying the hardware, at the first place, if this price is higher than reasonable.
Operating System	Choosing each hardware device of cybersecurity whereas considering the advantages and inconveniences of its operating system.
Amount of Interfaces and their throughputs	Choosing each hardware device according to the necessary amount of port interfaces for computers, servers, routers and switches whereas considering their throughputs of binary data.
RAM space	The hardware device must have an appropriate memory space of RAM (Random Access Memory) to enable it to process the expected amounts of TCP/IP packets.
Cores	The number of integrated cores within a hardware device of cybersecurity is reflected on its processing capacities.
Number of processors	The number of integrated processors within hardware products of cybersecurity is reflected on their processing capacities
Processing frequency	High processing frequencies at the level of hardware products of cybersecurity enable them to treat TCP/IP packets in high rates.
Firewall Throughput	A hardware firewall may integrate the functionalities of IPS, IDS, VPN (Virtual Private Network) and Antivirus. Therefore, the total throughput of a firewall, which may be expressed either in Megabytes per Seconds (MBps) or in Megabits per second (MbpS), defines the resulted capacities of processing TCP/IP packets after implicating the influences of frequency, RAM, cores and number of processors.
IPS Throughput	Total throughput of data at the level of IPS in Mbps or in MBps.
IDS Throughput	Total throughput of data at the level of IDS in Mbps or in MBps.
VPN Throughput	Supported throughput of data for a VPN, which may be expressed either in Mbps or in MBps.
AV Throughput	Supported throughput of data at the level of AV (Antivirus).
UTM Throughput	Supported throughput of data for UTM (Unified Threat Management), which may be expressed either in Mbps or in MBps.
Concurrent Connections	The number of parallel connections that can be processed and established simultaneously.
New Connections per second	The amount of new connections per second that may be supported and processed.
VLAN Support	Maximum number of supportable VLANs (Virtual Local Area Networks)
Authenticated User Limit	Maximum number of authenticated users that may access the configuration and functionalities of a cybersecurity device.
Branch Office VPN	Maximum number of supportable VPNs.
Mobile IPSec VPN	Maximum number of supportable mobile VPNs that include the use of IPSec (Internet Protocol Security).
Form Factor	The form of device (Desktop device, Server device, etc.).
Power Supply	Plug range of power supply and its type, which may be DC (Direct Current) or AC (Alternating Current).
Difficulty of deployment	A hardware product for cybersecurity may be difficult to deploy depending on its datasheets and procedures of installment, which may require specific skills in networks engineering.
Difficulty of configuration	The software of a hardware product dedicated for cybersecurity may be based on graphical configuration or textual code configuration.
Compatibility with other technologies	Networks of e-learning and online experimenting may include various technologies bought from different providers. Therefore, it is paramount to verify the compatibility of cybersecurity devices with these technologies.

hackers and web intruders by relying on standards of ISO/IEC 27033 and RIT. Therefore, we dedicate this section to determine the technical characteristics and financial criteria to choose appropriate products to establish solidified cybersecurity for e-learning platforms and online laboratories.

There are many aspects to analyze before considering any technological product to establish (or reinforce) the cybersecurity of e-learning platforms and online laboratories, which are as follow:

- The used hardware for web hosting.
- The used hardware for remote experimenting.
- The used software for content management and online experimenting.
- The size of deployed networks.
- The aimed number of online users to be supported.
- Deployed resources that rely on real-time serving.
- Deployed applications that may be accessible through internet.
- The financial funding to establish (or reinforce) the cybersecurity.

At the market, many technology providers are offering different prices for products varying according to their technical capacities. In Table 1, we present different product

Table 4: Technical characteristics and financial criteria to choose software products for cybersecurity.

Criteria	Description
Price per month	Necessary price to be payed each month to use a software of IPS, IDS, Firewall, VPN or Antivirus.
Price per year	Necessary price to be payed each year to use a software of IPS, IDS, Firewall, VPN or Antivirus.
Price per unit license	Necessary price to be paid for each computer or server on which we may install a cybersecurity software.
Total investment in software	Each purchased cybersecurity software should require the minimum financial dispenses over years.
Operating System	Each cybersecurity software is usually dedicated to specific operating systems.
Necessary RAM space	Each purchased cybersecurity software should require the least amount of RAM space, in order to avoid slowing computers and servers.
Necessary memory space on hard drive	Each purchased cybersecurity software should require the least amount of memory space on hard drives.
Included techniques of cybersecurity	It is advisable to purchase a software that may integrate different functionalities of cybersecurity, such as by purchasing a firewall software that includes also the functionalities of IPS software, IDS software, VPN and Antivirus.
Software Updating	It is advisable to purchase cybersecurity software from credible providers who offer persistent services of updating cybersecurity functionalities and updating the databases of virus signatures.
Autonomy of software	Each cybersecurity software should be autonomous, which means it can work independently form other software on computers and servers whereas all its integrated functionalities are working in coherence without latencies and without fells. In addition, these functionalities should not slow each other during the execution of their processes and should not slow down other processes on the same computers and servers.
Difficulty of installment	A software of cybersecurity may be difficult to install if it is dependent on other resources of software packages or if it requires complicated textual commands and bulky configurations to be installed.
Difficulty of configuration	A software of cybersecurity may be based on graphical configuration or textual code configuration.
Compatibility with computers and servers	Networks of e-learning and online experimenting are relying on different resources of software and hardware. Therefore, it is necessary to verify any software dedicated for cybersecurity with the capacities of these resources of hardware and software.

providers and hardware resources that can be relied-on to establish the cybersecurity of networks, whereas we present in Table 2 software products for the cybersecurity of networks and computer machines.

In Table 3, we present essential characteristics to choose hardware products for networks, whereas Table 4 is presenting the technical characteristics and financial criteria to choose software products for networks, computers and servers.

6. CONCLUSION

Technologies of e-learning platforms and online laboratories of experimenting are worldwide spreading by being deployed at the level of many educational establishments and institutions, which make it essential to define the implicated factors in the success of these technologies of e-learning and online experimenting. Therefore, this paper highlights the most influencing factors on the success of e-learning platforms and online laboratories at the levels of education, pedagogy, service providing, technology, marketing and management whereas promoting the necessity to enhance their cybersecurity. This paper also presents the necessary resources of hardware and software to establish this cybersecurity, whereas presenting the technical characteristics and financial criteria to choose them.

REFERENCES

1. A. Mynbayeva, Z. Sadvakassova, B. Akshalova. ***Pedagogy of the Twenty-First Century: Innovative Teaching Methods, in: New Pedagogical Challenges in the 21st Century***, Contributions of Research in Education, 2017.
2. A. Curtin, K. Hall. **Research methods for pedagogy: seeing the hidden and hard to know**, International Journal of Research & Method in Education, vol. 41, pp. 367-371, 2018.
3. T. D. Oyedotun. **Sudden change of pedagogy in education driven by COVID-19: Perspectives and evaluation from a developing country**, *Research in Globalization*, vol. 2, 2020.
4. WHO. Coronavirus disease (COVID-19) Pandemic. 2020. Available online: https://www.who.int/emergencies/diseases/novelcoronavirus-2019 (accessed on 25 October 2021).
5. WHO. Coronavirus Disease 2019 (COVID-19) Situation Report—51. 2020. Available online:

https://www.who.int/docs/defaultsource/coronaviruse/situation-reports/20200311-sitrep-51-covid-19.pdf?sfvrsn=1ba62e57_10 (accessed on 25 October 2021).

6. S. J. Daniel. **Education and the COVID-19 pandemic**, *Computers & Education*, vol. 49, no. 4, pp. 91-96, 2020.
7. O. B. Adedoyin, E. Soykan. **Covid-19 pandemic and online learning: the challenges and opportunities**, *Interactive Learning Environments*, pp. 1-13, 2020.
8. M. Aparicio, F. Bacao, T. Oliveira. **Grit in the path to e-learning success**, *J. Comput. Hum. Behav.* vol. 66, pp. 388-399, 2017.
9. S. Eom, N. J. Ashill, **A system's view of e-learning success model**, *Decision Sciences Journal of Innovative Education*, vol. 16, no. 1, pp. 42–76, 2018.
10. H. M. Selim. **Critical success factors for e-learning acceptance: Confirmatory factor models**, *Computers & Education*, vol. 49, no. 2, pp. 396–413, 2007.
11. J.J. Rodriguez-Andina, L. Gomes, S. Bogosyan. **Current trends in industrial electronics education**, *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3245–3252, 2010.
12. F. Esquembre, **Facilitating the creation of virtual and remote laboratories for science and engineering education**, *In 3rd IFAC workshop on internet based control education, IFAC-PapersOnLine*, vol. 48, pp. 49–58, 2015.
13. R. Heradio, L. de la Torre Cubillo, D. Galan, F. J. Cabrerizo, E. H. Viedma, S. Dormido. **Virtual and remote labs in education: A bibliometric analysis**, *Computers & Education*, vol. 98, pp. 14–38, 2016.
14. R. Heradio, L. de la Torre Cubillo, S. Dormido. **Virtual and remote labs in control education: A survey**. *Annual Reviews in Control*, vol. 42, pp. 1–10, 2016.
15. M. W. Rodrigues, L. E. Zárate, S. Isotani. **Educational data mining: A review of evaluation process in the e-learning**, *J. Telematics and Informatics*, vol. 35, no. 6, pp. 1701–1717, 2018.
16. J. Mtebe, C. Raphael. **Key factors in learners' satisfaction with the e-learning system at the university of dar es salaam, Tanzania**, *Australasian Journal of Educational Technology*, vol. 43, no. 4, pp. 75–86, 2018.
17. Y. Larbaoui, A. Naddami, A. Fahli. **Security, Control and Management of Smart Remote Laboratory for Remote Experiments in Electricity and Electronics**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 4068-4076, 2020.
18. Y. Larbaoui, A. Naddami, A. Fahli. **Switching Matrix Architecture For Flexible Remote Experiments Of Circuits Structuring In Electronics And Electricity While Using An Intelligent Algorithm**, *International Journal of Scientific & Technology Research*, vol. 10, no. 2, pp. 306-313, 2021.
19. Y. Larbaoui, A. Naddami, A. Fahli. **Online/Offline Web Services, Telecommunication and Management within Remote Labs, Universities and Research Centers**, *International Journal of Industrial Electronics and Electrical Engineering*, vol. 8, no. 2, pp. 16-21, 2020.
20. Garcia-Loro F. et al. **Educational Scenarios Using Remote Laboratory VISIR for Electrical/Electronic Experimentation**, *In: Auer M., Zutin D. (eds) Online Engineering & Internet of Things. Lecture Notes in Networks and Systems*, vol 22. Springer, 2018.
21. Y. Larbaoui, A. Naddami, A. Fahli. **Artificial Intelligent Algorithm to control Circuits Structuring of Flexible remote Experiments in Engineering within a Switching Matrix Architecture**, *International Journal of Emerging Trends in Engineering*, vol. 9, no. 2, pp. 92-102, 2021.
22. A. Minaeva, P. Šůcha, B. Akesson, Z. Hanzálek. **Scalable and e□cient configuration of time division multiplexed resources**, *Journal of Systems and Software*, vol. 113, pp. 44–58, 2016.
23. S. Faruque. ***Time division multiplexing (tdm)***, *in: Radio Frequency Source Coding Made Easy, Springer, pp. 91–118, 2015.*
24. Y. Larbaoui, A. Naddami, A. Fahli. **Adapting Hands-on Laboratory's Materials and Embedded Systems from Local Use to Remote Experimenting through Internet**, *International Journal of Innovative Science and Research Technology*, vol. 5, no. 7, pp. 518-528, 2020.
25. Y. Larbaoui, A. Naddami, A. Fahli. **Shared Hardware Resources through Internet for Remote Experiments in Electronics and Electricity**, *SSRG International Journal of Electrical and Electronics Engineering*, vol. 7, no. 10, pp. 1-11, 2020.
26. D. Lowe, S. Conlon, S. Murray, L. Weber, et al. **Internet accessible remote laboratories: Scalable e-learning tools for engineering and science disciplines**, *IGI Global*, pp. 453–467, 2012.
27. P. Orduña, P. H. Bailey, K. DeLong, D. López-de-Ipiña, J. G. Zubia. **Towards federated interoperable bridges for sharing educational remote laboratories**, *Comput. Hum. Behav.*, vol. 30, pp. 389-395, 2014.
28. Iso/iec 27033 (2015). [Online]. Available: https://www.iso27001security.com/html/27033.html (accessed on 25 October 2021).
29. Rit standards (2015). [Online]. Available: https://www.rit.edu/security/content/intro-policies-standards (accessed on 25 October 2021).