Research Article

Cyber Security Featuresfor National E-Learning Policy

Alya Geogiana Buja[1*], Noor Afni Deraman[2], Siti Daleela Mohd Wahid[3], Mohd Ali Mohd Isa[4]

[124]Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, Malaysia
[3]Faculty of Business Management, Universiti Teknologi MARA, Malaysia
geogiana@uitm.edu.my[1]

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: This paper proposes cybersecurity features in the National e-Learning policy. Cybersecurity in the learning environment is becoming an issue that has been considered by the community. DePAN 1.0 and DePAN 2.0 policies have not been carefully planned in any related security concerns. Amongst security domains in e-learning are authentication and accountability, access control, and non-repudiation issues. However, as the functionality of e-learning is expanding, information must be actively protected in this bigger context to avoid the loss of its confidentiality, integrity, and availability. Therefore, the existing policy and guidelines on e-learning have been studied thoroughly. A very feasible study has been conducted on the existing literature and related works to e-learning and e-learning. The security threats are also reviewed in this paper. Based on the established e-Learning policy, therefore, the proposed security features are namely (CSF1) authentication and accountability, (CSF2) access control, (CSF3) protection of communication, and (CSF4) non-repudiation issues. The findings from this study can be added to the implementation of e-learning in the future.

Keywords: Cybersecurity, e-Content, e-Learning, Security policy.

1. Introduction

The urged by the Ministry of Education (MOE) to switch the teaching & learning from the traditional classroom to advance online classes at higher learning institutions (HLIs) due to the pandemic crisis is an eye-opener to everybody. Statistically, 36% out of 86,672 students reported not completely ready for online-learning [1]. But the learning process must be continued. Due to the pandemic, many HLIs have also slowly changed over the last forty years in consideration of policy drivers, such as widening participation, long-life learning, and quality assurance [2]. The environment of the study has been migrated to Open Distance Learning (ODL). ODL is defined as a method of learning that more to self-learning which fully utilize the information technology and the Internet. The participants of e-learning have to share the learning and teaching materials on the Internet; accessible only at anytime and anywhere. The National e-Learning Policy (DePAN 1.0 and DePAN 2.0) [3,4,5] are very much needed as both are the guideline for e-learning environment in Malaysia.

However, the cyber-attack is increasing gradually with the evolvement of information technology. The demand for using the e-learning platform is high because of the changing teaching method and learning of all learning institutions worldwide. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. As such, information must be protected to avoid losing its confidentiality, integrity, and availability.

Several cyber-attacks could compromise the e-learning environment that might be harmful to the information and the user, such as spreading viruses and worms over the Internet. Besides, with the universal connectivity, unauthorized access or the user's data can be collected without their knowledge. For the learning and teaching material, the attack on intellectual property can happen. From time to time, the type of cyber-attack appears in a different form.

With that in mind, this paper proposes four cybersecurity features to be embedded in the National e-Learning Policy. In Section 2.0, this paper reviews the National e-Learning Policy, security issues in the e-learning system, and the relationship of E-learning and information security management. Section 3 briefly explains the method of this study, and Section 4 presents the proposed cybersecurity features of the National e-Learning Policy, and the conclusion is presented in Section 5.

2. Related literature

This section discusses related and relevant literature to the study. Section 2.1 reviews on National e-Learning Policy and Section 2.2 discusses security issues in the e-learning system. Meanwhile, Section 2.3 explains the relationship between e-learning and information security management.

A. National e-Learning Policy

In Malaysia, there are two existing policies related to e-learning implementation. Unfortunately, both policies have not cautiously investigated each domain's security assessment in the National e-Learning Policy, even in DEPAN 2.0 (refer Figure 1).

The first National eLearning Policy, or in the Malay language, Dasar e-Pembelajaran Negara (DePAN) was enacted in 2011 to provide a framework and direction for eLearning implementation in higher education. It focuses on collaborative learning, which became the teaching and learning philosophy and could even provide career options and much more [6]. Previously, DePAN 1.0 was constructed with five pillars: Infrastructure, Organizational Structure, Curriculum and e-content, Professional Development, and Acculturation. Later, DEPAN 1.0 has been revised to DEPAN 2.0 and enhanced with six pillars: Infrastructure and Infostructure, Governance, Online Pedagogies, e-Content, Professional Development, and Acculturation.

Shifting DePAN 1.0 to DePAN 2.0 is a never-ending story when ignoring the elements of information security. Information security is needed to protect all shared information from threats. With advanced technology, information can easily be manipulated, hacked, and stolen. Therefore, understanding the idea of information security is a must in executing ODL.

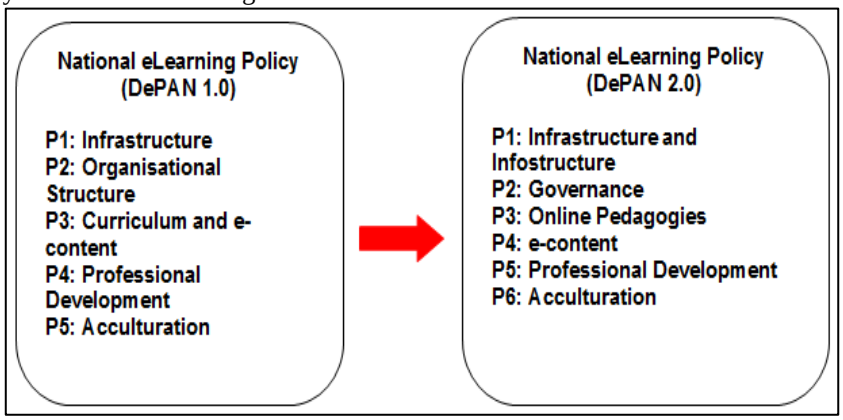

Figure 1: The National e-Learning Policy

B. Security Issues in E-Learning System

These past years, e-learning starts to proliferate. This large platform's elements enable us to share information, collaboration, and interconnectivity through the e-learning system. The community will face several threats and risks with the e-learning system [6]. As we knew, the authors wrote book journals and documents. Protecting their work from unauthorized use, modification, or reuse is their duty. Next, teachers should be more concerned about the risk of plagiarism, especially during the e-learning session, since everything is easy to access. Storing information like user ID and passwords allows hackers to access the students' data, so they should beware and ensure themselves not entering any confidential information at unauthorized websites. In addition, managers also will face risks like this. To be safe, ensure there are backup plans for everything, and every copyright is secured.

Some countermeasures and solutions in improving e-learning security are developed to cope with the increasing threats. It becomes more secure with the help of the existence of new technologies. Cryptography is one of the initiatives where the data and information are converted to scrambled and unintelligible format to ensure information safety. Furthermore, digital right management allows authors and artists to control people's access to their creations. Next, a distributed firewall solution is where security software applications protect the enterprise network servers and end-user against unwanted elements. Other than that, biometric authentication is also one of the initiatives. As an instance, authentication techniques such as requesting passwords, pins, and ID. Finally, it is by using digital watermarking. This method allows the owners to add copyrights to protect their works against unauthorized use.

In addition, authentication can prevent identity theft during authentication. Firstly, a reply attack where sensitive information is compromised becomes useless to the theft. Next, social engineering attacks. The system could guarantee that all of the credentials cannot be transferable. Shoulder surfing attacks are where the information gained by the attacker does not result in anything. In addition, ensure installed malware does not affect the models even there is a replay attack. Ensure that attackers cannot copy the authentication interface even after observing any successful authentications or can be called a phishing attack. Eavesdropping resistance and authentication code reformation and reuse also contribute to security problems [7]. There are some others such as high entropy, user friendly interface, physically harmless, memorability and quick training, which are also some of the elements that contribute to preventing attacks. Hence, there are various ways of ensuring our data is secured during the e-learning system.

C. E-Learning and Information Security Management

Security for e-learning should be taken seriously and always implemented to ensure that a secure e-learning environment is built. The growth of e-learning opens a new path and generation of learning styles. It also led to a significant opportunity for the community to become learners. In this era, everything is at the fingertip, which enables everyone to access everything easily. However, there are also some consequences to it. It leads to illegal activities such as leaked personal information. To conceal this problem, information security management needs to be upgraded.

Many web applications and medium are used as a platform for e-learning and lead to the cases of Internet attacks. Plus, the information security in e-learning are always neglected in any research. The potential of information security management also being discussed in the reference article.

E-learning is a term used to picture the usage of Internet technologies in enhancing teaching and learning. There are various definitions of e-learning can be found. E-learning started to develop bigger and meet many expectations. The bigger the growth of the e-learning environment, it will expose it more to information security threats. Either than security problems, these platforms also benefit in many ways, such as improving the quality of learning, reducing cost, save money and time.

Several challenges need to be faced when implementing e-learning. The challenges come from different perspective which are from the-learning provider or user perspective. Looking through the-learning provider perspective, the difficulties faced are mostly related to technical issues such as preparing efficient modules, delivering high bandwidth content like videos, content quality reduction, or even its cost. Meanwhile, from the users' perspective, the problem is on readiness, commitment, and skills. Besides that, low computer knowledge, self-discipline, and no self-learning initiative also lead to this problem.

Information exists in a variety of forms, whether hardcopy or softcopy. Whatever form it is, it should be secure. To keep its confidentiality and prevent integrity loss, security is necessary. The e-learning users can ensure their data information is protected with the availability of information security. The most common threats faced by e-learning are fabrication, modification, interruption, and interception. There are three areas focused by the researcher to avoid this kind of problem, which are policy, identities and intellectual property. To identify a legal user, authentication and authorization is recommended. This could help in controlling access from any other resources, than the user itself. Hence, information security is significant to keep the e-learning implementation secure.

Many information systems developed are not secure. Its security is limited, where it only can be achieved through technology. Security management is a discipline where it takes controls in the system. By implementing Information Security System (ISM), it can be controlled. ISM has its standards and outline to be followed [2]. The business needs and objectives also influence it. ISM is almost similar to other e-services but also have some difference in the offered services. The E-learning platform is flexible and ensures the confidentiality, availability, and integrity of information. The user's behavior in e-learning is different from a user of other e-services. Therefore, ISM existence in e-learning is significant.

3. The methodology

This study is conducted in three phases: feasibility study, threat analysis, and cybersecurity feature identification. During the feasibility study, the National e-learning Policy was studied thoroughly by looking and analyzing each pillar's security element. Based on the study, not all pillars can be embedded with the security features. For DEPAN 2.0, three pillars have been identified that can be improvised with the cybersecurity features, which are P1 - Infrastructure and Infostructure, P2 – Governance, and P4 - e-Content.

Once the suitable pillars have been identified, all related information about the pillars is gathered. The purpose of this activity is to identify the security threats that can be happened in the e-learning ecosystem if the pillar is not secure.

Lastly, based on the threat analysis, the cybersecurity features are proposed.

The proposed cyber security features for national e-learning policy

To produce the guideline of learning environment, the method of how to implement, monitor, and review and improve has to be taken into consideration to ensure that the specific security and business objectives of the organization are met. Besides, the control of the environment has to be identified carefully and explained clearly in the policy. This can be done by supporting the technical elements with appropriate management and procedures [8].

As shown in Figure 2, the Open Distance Learning (ODL) scenario, it is principally demanding attention in the domain of cybersecurity features, namely (CSF1) authentication and accountability (CSF2) access control, (CSF3) protection of communication and (CSF4) non-repudiation issues. The enforcement and practice of cybersecurity must be together with the e-Learning policy because the e-Learning policy comprises of pillars that might be vulnerable and can be compromised by intruders. Figures 3, 4, and 5 show pillars that must be facilitated with cybersecurity features.

A. Authentication and Accountability

Authentication provides a way of identifying a user and is a fundamental process for ODL since there are numerous numbers of platforms used to implement ODL. One of the main platforms necessary for implementing ODL is the use of a Learning Management System (LMS). LMS is used to share information with students, have an online discussion, assignment submission, and conduct assessment.

Usually, users are required to enter a username and password before being granted access to the LMS. This is just one of the three ways to authenticate a user: knowledge-based authentication, which requires users to provide something they know. Authentication can also be done via token-based, which requires users to provide something they own, such as a mobile device or key card. Finally, authentication can also be done by user providing something that can be measured such as fingerprint, palm print or retinal image. Amongst all the three authentications method, passwords are the most widely used [7].

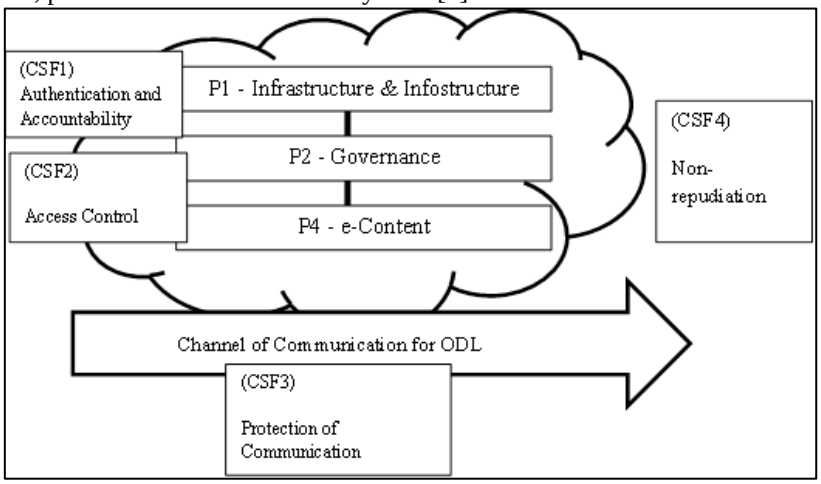

Figure 2: Proposed Security Features for National e-Learning Policy

This poses a problem because as technology advances and attackers become smarter and technologically savvy, using a password makes intrusion very achievable for the attacker since learners have a problem remembering a long and complex password. They often resort to using simple password [7]. Clearly, a solution that not dependents on a password alone but also utilize current technology is needed for LMS.

One possible solution is by enabling the use of Two (2) Factors Authentication (2FA) during the login process. During 2FA, users are sent code to their mobile phone, which is required for authentication; this code is required to be submitted along with the username and password.

This adds another layer of security, even if the password was compromised. Those who may have problems with internet access or connection can also opt to use a 2FA authenticator app such as Google Authenticator or Authy, which uses time-based to generate code instead. According to Google, by adding 2FA alone will block 100% automated bot hacks [9], which is one of the automated attacks carried out by attackers to gain access to an account.

Although it is clear that 2FA is necessary to improve authentication, many LMS are still behind in implementing 2FA. Based on the list at [10], which reviews the top 10 learning management systems (LMS), only 4 out 10 LMS currently support 2FA: Moodle, Canvas, Blackboard and Google Classroom. If we look further at twofactorauth.org (2020) , which list website support for 2FA, there are still many websites related to online-learning that still have no support for 2FA, such as Coursera, Edmodo, edX, and Udemy.

Hopefully, this trend will change, and more LMS will start to support the use of 2FA since an online-learning authentication is very important because it relates to the second component of security, which is accountability. Accountability refers to the ability to tie user with the action performed by the user. So that we can be sure that it is the user that submitted the assignment or takes the online assessment.

B. Access Control

As with any other online system, users are given privileges based on their account. These privileges are generally tied to the role given to the user. The role will then determine the action that can be carried out by the users, also known as access control or role-based access control, since the role will determine the level of access.

In older versions of LMS and in most cloud based LMS, a fixed set of roles was used to simplify the LMS usage [11]. These roles are normally separated into three groups, which are administrators, teachers, and students, and no new roles can be created. This generalization of privileges is problematic because it does not allow fine-grained control of users' permission. For instance, an administrator would normally be given all access to the system and is given too much control. Perhaps the administrator can be grouped into administrator for user, administrator for the course, and administrator for faculties. This limit in access will control the amount of access that a user has when an account is compromised.

Newer versions of LMS such as Moodle and edX allow finer control of permissions to be assigned to a newly created role. This should be able to overcome the problem with a compromised account having all permissions. Care though should be taken when creating a new role and when assigning tasks to the role. Some of the security that may arise with the wrong permission setting is (i) users are allowed access to other users' confidential data or (ii) users can send messages to all users, which may contribute to spamming. A balance access control is essential in e-learning to ensure that users are given the right permission to accomplish their tasks.

Domain	Focus Area	Phase 1 (2015)	Phase 2 (2016–2020)	Phase 3 (2021–2025)
Infrastructure & Infostructure	Internet & Wi-Fi Coverage	1–5 Gbps Internet access (streaming of SD videos)	6–10 Gbps Internet access (streaming of HD videos)	Minimum 10 Gbps Internet access (streaming of full HD videos, tele-presence)
		1 Mbps/student and 80% coverage	2 Mbps/student and 90% coverage	2.5 Mbps/student and 100% coverage
	eLearning Platform	eLearning platform 2.0 and MOOC-ready	eLearning platform 2.0 MOOC- and mobile-ready	eLearning platform 2.0 MOOC-, mobile- and learning analytic-ready
	ICT Equipment and Software	100% of lecturers and 90% of students have computer / notebook / tablet / smartphone	100% of lecturers and 95% of students have computer / notebook / tablet / smartphone	100% of lecturers and 100% of students have computer / notebook / tablet / smartphone
		50% of lecturers have access to e-content development software	75% of lecturers have access to e-content development software	100% of lecturers have access to e-content development software

Figure 3: P1 - Infrastructure & Infostructure

Domain	Focus Area	Phase 1 (2015)	Phase 2 (2016–2020)	Phase 3 (2021–2025)
Governance	Policy & Action Plan	eLearning policies formulated and adopted holistically	eLearning policies are updated per current demands in terms of the use of new technology, ethics and copyright	eLearning policies are harmonised with the standards of international eLearning policies
		HEI has comprehensive eLearning action plan	HEI implements the comprehensive eLearning action plan	HEI harmonises the action plan with international standards
	Leadership & eLearning Unit	eLearning leadership has the latest skills and is recognised at the institutional level	eLearning leadership has the latest skills and is recognised at the national level	eLearning leadership has the latest skills and is recognised at the global level
		eLearning Unit is established and fully operational	eLearning Unit collaborates in eLearning activities at national and regional levels	eLearning Unit collaborates in eLearning activities at the regional and international levels
	Human Resources & Financial Allocation	HEI has human resources and appropriate staffing to carry out all eLearning activities	HEI provides training, certification and career paths in human resources related to eLearning	Human resources related to eLearning acquire international certification
		HEI allocates 0.5% of the annual operating budget for the implementation of eLearning	HEI allocates 1.0% of the annual operating budget for the implementation of eLearning	HEI allocates 1.5% of the annual operating budget for the implementation of eLearning

Figure 4: P2 - Governance

C. Protection of Communications

In traditional online learning, communications are normally carried out in an asynchronous mode via chat module or discussion in the LMS forum module. This is due to limitations of available bandwidth in delivering voice or video. So then, the security of communications depends on the security of the database in protecting the data.

As technology advance and more bandwidth are available for both home users and mobile users, online classes and discussions can be performed synchronously between teachers and students. Although the video conference platform has been around since the 90s, Webex for instance, was launch in 1995, the pandemic has created a demand for an easy to use video conferencing software. Some of the well-known video conferencing software are Webex, Microsoft Teams, Google Meet, and Zoom.

This led to security problems because since users must install the applications on their devices, the applications may have some vulnerability that will expose the device to attackers and later be compromised. List of vulnerabilities includes:

a. Remote code execution (RCE) is where attackers can execute code on the remote machine and ultimately have complete access and control to the machine.

b. Session hijacking – vulnerability allows attackers to send messages that will perform certain actions such as sending messages on behalf of the users, removing the users from the meetings, or even hijacking the screen being shared [12].

c. Zoombombing is also known as zoom raiding. It is when unwanted users (normally internet trolls or hackers) can join a video conference call and hurl racial slurs, profanity, or even shares offensive images. Although this is not a software security vulnerability, it is still a problem with how Zoom handles public meeting links [13].

d. Eavesdropping – this is the ability of attackers to listen to the conversation.

e. Privacy – since some video conferencing applications are offered free to users, the company often makes money by mining user data. This may be of concern if a company or organization uses the application.

As we can see above, many issues come with the popularity of video conferencing software; as a guide, we would like to offer the following recommendations to users:

a. End-to-end encryption – Some applications provide supported for E2E, which means that the encryption is between end devices to another end device. Any intermediary device or node along the communications channel will not be able to eavesdrop on the conversation. It is highly recommended that applications that support E2E are used.

b. Keep the software updated – Always enable automatic checking of an update for the software and update it when an update is available.

c. On-demand installation – If the software is only used for a few times a week, one can install the software when required and uninstall it once it has been used. This will minimize vulnerabilities causes by remote code execution.

As with any other software category, video conferencing applications will soon become mature and contain fewer vulnerabilities. Until then, users are advised to take extra precautions when using the software.

D. Non-repudiation

In an online transaction, it is essential that a user can be held responsible for the action that they had carried out. In cybersecurity, this is known as non-repudiation, which provides proof of the origin of the data and its integrity. Certain activities in ODL require non-repudiation to be implemented, especially for activities that influence grading, such as submitting an assignment or taking a quiz. Hence logging mechanisms that record all users' activities are required.

However, most of the loggings rely on user authentication and access-control to link users to their respective activities. This may not be adequate since an action can be carried out by a compromised account, which may unfairly punish the user. Also, non-repudiation can also occur outside of the LMS, such as users sharing confidential materials to the public. As a recommendation, it is suggested that the following are implemented:

a. For administrators, critical activities such as adding, editing, and removing users are recorded as well as generating triggers for other administrators. This is so that the actions can be evaluated later by others if a problem arises.

b. For assignment submission or answering the quiz, digital signatures can be used to ensure the submission's integrity.

c. For unauthorized distributions of materials, digital watermarking can be used to track the person responsible.

By following the guide above, we should minimize the security issue related to the repudiation attack.

Domain	Focus Area	Phase 1 (2015)	Phase 2 (2016–2020)	Phase 3 (2021–2025)
e-Content	Original e-Content	10% of all courses offered have original e-content	25% of all courses offered have original e-content	40% of all courses offered have original e-content
	Open e-Content	5% of all courses offered by public HEIs are developed and offered to the public (OCW)	10% of all courses offered by public HEIs are developed and offered to the public (OCW)	15% of all courses offered by public HEIs are developed and offered to the public (OCW)
	e-Content Standard	e-Content standards are established	e-Content standards are enforced	e-Content standards align with international standards

Figure 5: P4 - e-Content

4. Conclusion

In conclusion, this paper presents the cybersecurity features in the National e-Learning policy. Due to the COVID-19 pandemic, e-Learning has been taken into consideration by all learning institutions worldwide. This study has feasibly studied the National e-Learning Policy and found that the security features could be added to the policy. E-learning requires a cyber platform to execute the business process, and the platform has to be secured for the users to communicate the data. Therefore, four cybersecurity features have been proposed in this paper, namely (CSF1) authentication and accountability, (CSF2) access control, (CSF3) protection of communication, and (CSF4) non-repudiation issues with hardening the three pillars; P1 - Infrastructure and Infostructure, P2 – Governance and P4 - e-Content. The proposed cybersecurity features have been analyzed in terms of the implementation based on the identified pillars of the National e-Learning Policy. For future work, the next step in this research project is to conduct the preliminary survey to obtain the effectiveness of the proposed enhancement of cybersecurity features in the National e-Learning Policy.

Acknowledgements

Sincere appreciation goes to Universiti Teknologi MARA Cawangan Melaka for the support given to this research endeavor, TEJA: Internal Grant (GDT2020-17).

References

1. Bahagian Hal Ehwal Akademik. (2020). Laporan Ketersediaan Pelajar Bagi Pembelajaran & Pengajaran Dalam Talian Universiti Teknologi MARA.
2. Najwa Hayaati, M.A. & Ip-Shing, F. (2010). E-Learning and Information Security Management. International Journal of Digital Society, 1(2), 148-156
3. Dasar e-Pembelajaran Negara. Retrieved at http://www.ukm.my/jurutera/wp-content/uploads/2016/07/e-Pembelajaran-Negara.pdf on 10th of May 2020.
4. Dasar e-Pembelajaran Negara 2.0. Retrieved at http://www.cade.upm.edu.my/dokumen/PTPA1_DePAN_v2.pdf on 10th of May 2020.
5. Ministry of Education Malaysia. (2020). Malaysia education blueprint 2015–2025: Executive summary.
6. Buletin Pembangunan Akademik UKM (2011). Retrieved at http://www.ukm.my/ctlt/wp-content/media/Bulletin/PPA_bil_6.pdf on 10th of May 2020.
7. Salimovna, F., Yuldasheva, N. & Ugli, I. (2019). Security issues in E-Learning system. 1- 4. 10.1109/ICISCT47635.2019.9011971.
8. Rozhan, M.I., Nurkhamimi, Z., Najwa Hayaati, M.A. Ahmad Farid, M.J. & Eznie Zahirah, M. (2017). Towards National Policy Guidelines on Open Educational Resources in Malaysia. Vancouver, Canada: Commonwealth of Learning. pp: 1-57.
9. Anonymous. (2020). Two Factor Auth (2FA) (2020). Retrieved at https://twofactorauth.org/#education
10. Fenton, W. (2018). The Best (LMS) Learning Management Systems for 2018.
11. 11. Skripak, I. A., Aynazarova, S. N., Vladimirovna, E., Tkachenko, A. E., & Erina, L. S. , Digital Virtualization Technologies in Distance Learning, Advanced Trends in Computer Science and Engineering Available, 9(2), 1808–1813, 2020. Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse138922020.pdf
12. Thomas, K., and Moscicki, A. (2019). New research: How effective is basic account hygiene at preventing hijacking. Retrieved at https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html.
13. REISINGER, D. (2020). Zoom Bug Gives Hackers Full Control Over ComputersWorse yet, there's apparently no fix. Retrieved at https://www.inc.com/don-reisinger/zoom-bug-gives-hackers-full-control-over-computers.html.