Cybersecurity in E-learning Systems

Alhumaidi Alderaan.

Computer Trainer, Aljouf Technical College,

Technical and Vocational Training Corporation (TVTC), Saudi Arabia

Email: a.alderaan@outlook.com

Abstract

This paper aimed to review the challenges and issues related to cyber security in e-learning systems. A Google Scholar search yielded 18 papers for review. These were discussed in various sections. The review helped to appreciate the complexity of e-learning systems and their dependence on the internet makes them vulnerable to cyber security threats. Especially, as e-learning became the new normal due to the impact of the covid pandemic, this risk still exists and increasing. Despite all the advantages of e-learning, since it uses the internet, e-learning systems are prone to cyberattacks. The review also informed about the types of cyber-attacks on e-learning systems, solutions to the challenges of cyber security, models and frameworks of cyber-attacks and security issues and the benefit-cost aspect.

Keywords: Cybersecurity, e-learning systems, review of literature

Introduction

E-Learning is widely used as a method of learning, in which the internet is used for both delivery and access to learning sources. The computing systems, networks and the internet provide a complex system for e-learning. E-learning aims to guarantee the satisfaction of the learner and maintain a good image of the learning process. Due to its anytime anywhere capabilities, e-learning provides many opportunities for students, trainees and educators to acquire, develop and maintain core skills and essential knowledge. In the current covid pandemic, e-learning rescued educational institutions from breakdown of the academic programmes to a great extent. Despite all the advantages of e-learning, since it uses the internet, e-learning systems are prone to cyberattacks. This review aimed to evaluate some of the available literature on the issues related to e-learning systems.

Methodology

Appropriate search terms were used in Google Scholar to identify and select the literature relevant to the topic. Only those published in English from 2014 to 2021 were selected. Although full texts were selected to the maximum extent, if abstracts only were available, they too were included if some important points were made in them. This strategy yielded 18 papers for this review. These are discussed in the following sections.

Results

The nature of e-learning

The Blackboard e-learning system components, requirements, merits and examples of successful applications in universities were discussed by eM Elsawy and Ahmed (2019). E-learning is offered at the basic, blended (traditional and e-learning combined), full and advanced levels. E-

learning can be used for training, continuing education, providing resources and development of knowledge and skills, and providing opportunities for women for education in countries where their level of education is low. E-learning provides an equitable chance for the education of all, accessibility at anytime and anywhere and supports collaborative learning among students and promotes self-education. E-learning can be synchronous or asynchronous. In synchronous e-learning, the teacher meets the learners simultaneously for simultaneous communication and virtual classes. In asynchronous e-learning, a teacher may provide resources for teaching and evaluation plans on the learning management system. The student enters at any time and follows the teacher's instructions to complete the learning without simultaneous communication with the teacher on tasks or discussions. Successful e-learning experiences from some universities in Abu Dhabi and Saudi Arabia have been presented.

Nature of cyber-attacks on e-learning systems

The cybersecurity issues in e-learning were generally reviewed by Bandara, Ioras, and Maher (2014). Ensuring the cybersecurity of e-learning systems is a unique challenge. This is because numerous systems are accessed and managed via the internet by thousands of users over hundreds of networks across a wide region. Many times, a lack of clear IT policies can lead to the prevalence of internal cyber-attack. This affects the various procedures in e-learning systems and their architecture, violating their specific security requirements. The authors discuss an approach to understanding, evaluating, monitoring, measuring and managing the cybersecurity of e-learning systems. The policies like Bring Your Own Device (BYOD) can lead to increased risk of cybersecurity. The highest cybersecurity arises from BYOD, viruses, social media, virtualisation of computers and servers and consumerism. Threats due to inadequacies of authentication, availability, confidentiality attacks and integrity attacks also occur. The security issues in e-learning are listed below-

- Deliberate software attacks (viruses, worms, macros, denial of service).
- Technical software failures and errors (bugs, coding problems, unknown loopholes).
- Acts of human error or failure (accidents, employee mistakes).
- Deliberate acts of espionage or trespass (unauthorised access and/or data collection).
- Deliberate acts of sabotage or vandalism (destruction of information or system).
- Technical hardware failures or errors (equipment failure).
- Deliberate acts of theft (illegal confiscation of equipment or information).
- Compromises to intellectual property (piracy, copyright, infringement).
- Quality of Service deviations from service providers (power and WAN service issues).
- Technological obsolescence (antiquated or outdated technologies).
- Deliberate acts of information extortion (blackmail for information disclosure).

As e-learning expands, the internet also expands to cover more areas and broader aspects of our education, cybersecurity has become the major concern concerning privacy protection, authentication of transactions, and confidentiality of user information stored in a database server. Hackers usually release attacks to steal confidential data from organizational database servers. Hence, it is very important to place strong security measures for the protection of the data and information of the end-user against any malicious attack. The cybersecurity threats of e-learning, as tabulated by Ibrahim, Karabatak, and Abdullahi (2020) are given in Table 1.

Table 1. Security threats and categories of e-threats (Ibrahim, Karabatak, & Abdullahi, 2020).

Security Threats	**Categories of E-threats**
Worms, macros, denial of service	Deliberate software attacks
Bugs, programming errors, Undetected loopholes	Technical software failures And errors
Employees' mistakes, accidents	Acts of human error or failure
Unauthorized access, data collection	Deliberate acts of espionage or trespass
Destruction of information or system	A deliberate act of sabotage or vandalism
Equipment failure	Technical hardware failures or errors
Illegal confiscation of equipment or information	Deliberate acts of theft
Privacy, copyright, infringement	Compromises to intellectual property
Power and WAN service issue	Quality of service deviations from a service provider
Antiquated or out-dated	Technological obsolescence
Blackmailing for information disclosure	Deliberate acts of information extortion

Identity theft has been widely reported in respect of e-learning systems. This is due to increasing information sharing in social network sites (SNS) and e-learning systems (ELS). True awareness of these risks is not common among the users of SNS and ELS. Ball, Ramim, and Levy (2015) surveyed the effect of personal information sharing awareness (PISA) of users on their habits (PISH) and practices (PISP), while comparing the three constructs between SNS and ELS. The results of 390 responses showed that the users' habits had the strongest influence on their practices.

E-learning system such as Blackboard has several fantastic features that would be valuable for use during the covid pandemic. Almaiah, Al-Khasawneh, and Althunibat (2020) cited the works of Kwofie and Henten (2011), Ozudogru and Hismanoglu (2016), Almaiah and Almulhem (2018), Mtebe and Raisamo (2014), Almaiah and Alyoussef (2019) Almaiah and Man (2016) as reasons for the failure of e-learning systems due to lack of security and privacy concerns. Semi-structured online interviews (due to covid restrictions) with 30 students who have non-technical backgrounds and 25 faculty members, 4 IT experts and developers at five universities and 2 policymakers at the Ministry of Higher Education of Jordan were conducted through the Blackboard system. Their responses were thematically analysed using NVivo. The critical challenges and factors of e-learning usage identified from the interview responses were presented diagrammatically by the authors, as given in Fig 4. Security was one of the factors to adopt the e-learning system.

Figure 1 Critical challenges and factors of e-learning usage *(Almaiah, Al-Khasawneh, & Althunibat, 2020).*

Cloud-based E-Learning reduces the cost and complexity of data accessing, but is controlled by third-party services. When the traditional e-Learning methods are incorporated with cloud computing technology, it provides massive advantages to the e-learning system users, but at the cost of security. Durairaj (2015) identified different security issues in the cloud service delivery model aimed to suggest a solution of security measures in cloud-based e-learning. Different types of attacks in service delivery models of e-learning occur. Threats, security requirements, and challenges involved are considered when offering solutions. The final suggestion is for users to access their data in the cloud only through a secured layer using the internet. The authors cited an IDC report in which security is the highest-rated challenge in the cloud-on-demand contexts. Various types of cyber-attacks occur at SaaS, PaaS and IaaS levels of the cloud. In the proposed

system, there is a distinct security layer in the cloud, which can be used as the point of connection between the user and the cloud. A major obstacle in accessing cloud data for e-learners is data availability. Distributed Denial of service (DDoS) attack is related to this problem.

Overcoming cyber security challenges of e-learning

Most of these can be overcome by installing firewalls and anti-virus software, implementing security management (ISM); improving authentication, authorisation, confidentiality, and accountability; using digital right management and cryptography and training security professionals. Cybersecurity information governance for e-learning in higher education institutions can be visualised as given in Fig 1 (Bandara, Ioras, & Maher, 2014).

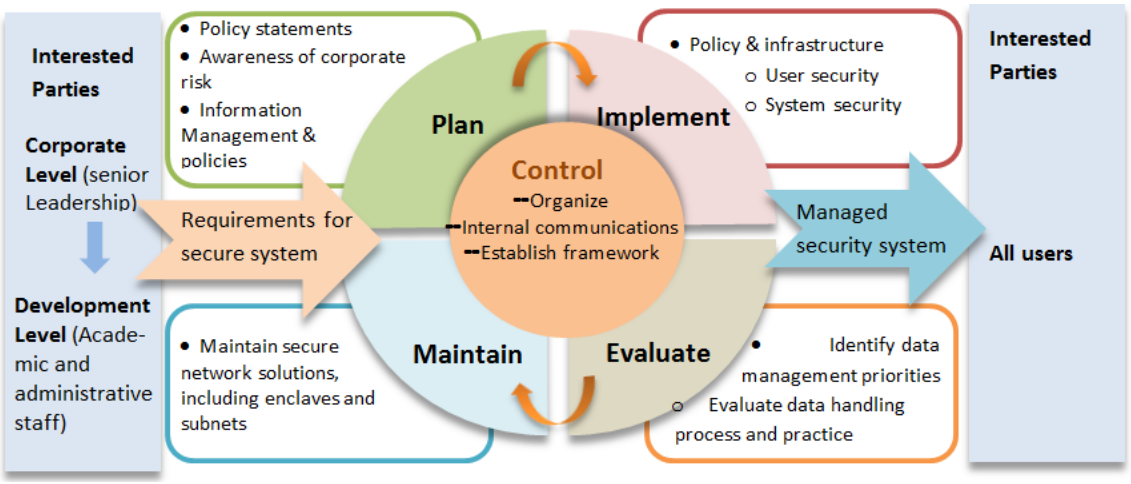

Figure 2 Cybersecurity management system for higher educational institutions *(Bandara, Ioras, & Maher, 2014)*.

In Fig 1, a plan-implement-maintain-evaluate framework has been used. Three management levels at interested parties, corporate and development levels determine requirements for a secure system, support it with policies, recognise risks and maintain secure network solutions. The outcome is a managed security system for all users with the required policies and protections. The system needs to be evaluated regularly as rapid developments in technologies can lead to fresh threats.

The management of cyber security issues in e-learning systems using BYOD was discussed by Anghel and Pereteanu (2020). The authors stress on information protection and data privacy depend on those security policies but also awareness among individuals regarding vulnerabilities, threats and risks. Policies need to focus on all devices with internet connection and individuals must know about both the benefits and risks of using BYOD.

A secure database management system model will have layers of protection at the system, functional, interface, and application levels. The management strategies of the secure database will consist of database privileges and access controls, database license, the establishment of data security using system-stored procedures, security as a database role, systematic installation of password vulnerabilities, patches, service packs and hotfixes, permissions and settings of operating systems, data encryption, audit trails and monitoring database access and data backup.

An e-learning data management system for security is given in Fig 2 from Ibrahim, Karabatak, and Abdullahi (2020).

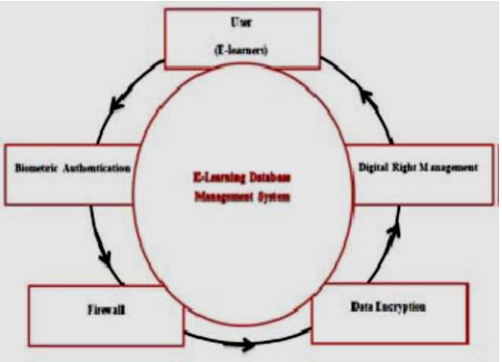

Figure 3 A process model to manage cyber threats on an e-learning system *(Ibrahim, Karabatak, & Abdullahi, 2020).*

As shown in Fig 2, such a management system will have user (e-learner) authentication, biometric authentication, digital rights management, firewall and data encryption as the protection layers.

The growing importance of a secure e-learning ecosystem became evident from DDoS (Distributed Denial of Service) attacks on e-learning components of the Croatian e-learning system. The negative impact of the attack was visible to numerous users. They were prevented from participating in and implementing the planned teaching process. Network anomalies such as DDoS attacks were identified as one of the crucial threats to e-learning systems. Anomalies in network traffic can indicate DDoS attacks. Denial of access to the IC service, system, or any resource to legitimate users is how DDoS happens. The concept of a botnet as a network of remotely managed vulnerable devices is well-known. Creating a botnet requires the implementation of malicious software in a target device that will allow remote management. The covid pandemic highlighted the importance of the availability of e-learning systems and services. Almost all educational institutions had to switch to e-learning. On March 16th, 2020, a DDoS attack on the AAI@EduHr system was responsible for authenticating the users to access various e-learning services in Croatia. After discussing the above points, Cvitić, Peraković, Periša, and Jurcut (2021) proposed a methodology to develop a DDoS traffic detection model. The UML diagram of this proposal is given in Fig 3.

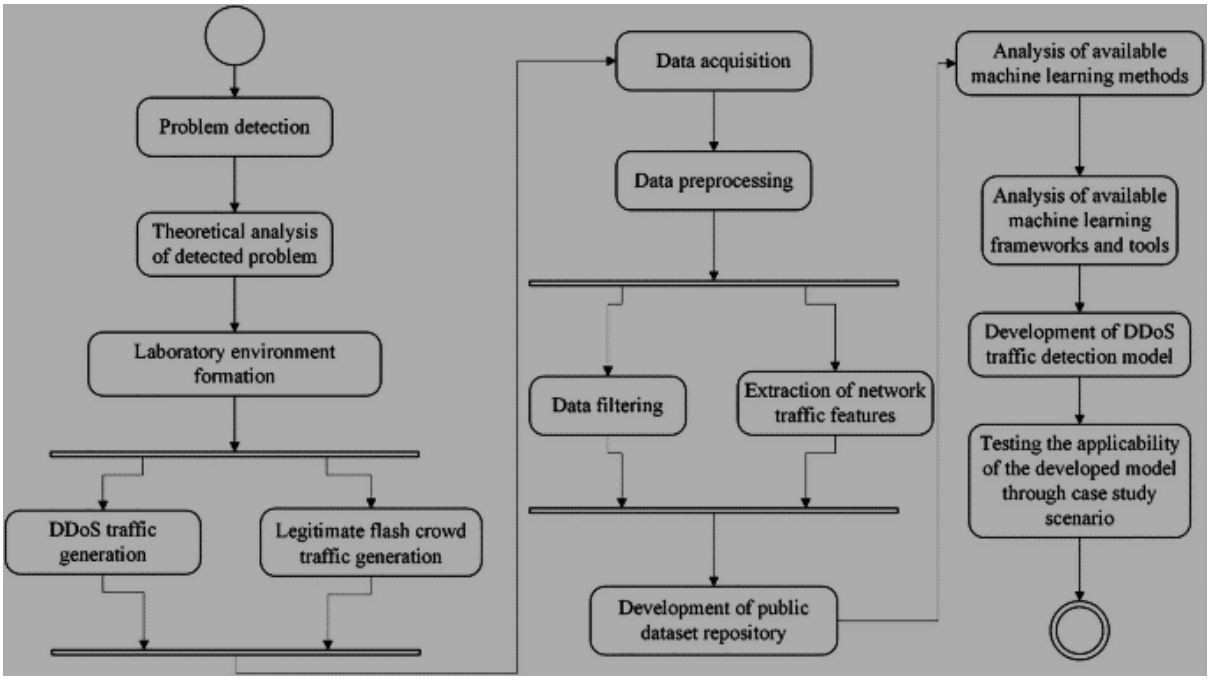

Figure 4 UML diagram of the methodology to develop a DDoS traffic detection model *(Cvitić, Peraković, Periša, & Jurcut, 2021)*.

The e-learning material provided for computer security training usually are similar to one another and do not consider the learning styles of the individual learners. Alshammari, Anane, and Hendley (2015) Proposed an approach to learning style adaptivity is for the teaching of computer security for more personalised and adaptive learning, based on the information perception style of the Felder-Silverman model. An experiment with 60 participants validated the approach of the authors. In teaching computer security via e-learning systems, matching computer security learning material, to the learning style of the students resulted in much better learning outcomes and student satisfaction than without matching them.

In the context of the covid pandemic forcing higher educational institutions to e-learning systems, the widespread use of cloud, computing, online platforms and videoconferencing posed high levels of cybersecurity threats in the form of DoS / DDoS attacks, cross-site scripting, spoofing, unauthorized data access and infection with malicious programs, and the theft of personal data. Alexei and Alexei (2021) tried to identify the causes of the attacks with significant impacts on the assets and the implications. Based on the results, updating systems and managing security patches, implementing access policies at the application or resource level, classifying information, and using cryptographic protocols were recommended. The published data on these aspects were analysed for reaching the above conclusions and recommendations.

In e-learning systems, a large amount of data is shared among students, teachers, and examiners. Although many clustering-based schemes are available to ensure cybersecurity, a dependable security system still evades research. Kausar, Huahu, Ullah, Wenhao, and Shabir (2020) examined a Secure E-learning System (SES) for sharing examination-related materials. Protection against various security attacks was ensured. Examination materials included tests, quizzes, question papers, answer sheets, and aptitude tests. A secure authentication mechanism was introduced for students and teachers with a trusted server or a fog server in the first phase. In

the second phase, a Session Key Establishment Protocol (SKEP) was provided to set up keys for a specified period such as a class, seminar or exam. The levels of trust and authentication were checked and maintained for the legitimacy of the students. A security analysis was done to identify the pros and cons of security schemes to ensure reliable security for e-learning systems. Results using a testbed on web services in ASP.net and C# on windows Azure cloud for an e-learning scenario showed the effectiveness of the proposed SES in reducing the number of untrusted students, exams exposed, student interaction time, authentication level, reputation and trust levels for students.

Recognising that cybersecurity is one of the major concerns of online e-learning systems, Farid, Ahmad, Alam, Akbar, and Chang (2018) included the minimum required measures of this aspect in the model proposed. Security was included as a part of the service quality in the network. However, the proposed model does not say anything new.

Cyber security awareness

To provide awareness of cyber security to e-learning students, it is necessary to know the current status of their awareness. The results of a survey conducted by Tirumala, Sarrafzadeh, and Pang (2016) with this aim showed low levels of awareness among students in the age group of 8 to 21 years. The level was much lower in the case of the subgroup in the age range of 8 to 12 years. Most of the students were not familiar with common cybersecurity terms or the common cybersecurity threats like phishing and security tools to be used for tablets and smartphones, the two most frequent BYOD devices. Thus, the need to provide awareness among students was established.

Cybersecurity models/frameworks

Realising that the current cyber security awareness training programs rely on manual setup and configuration with hands-on activities, which itself is prone to cyber-attacks, Beuran, et al. (2017) implemented the CyTrONE, an integrated cybersecurity training framework, to address such shortcomings. The framework was intended to automate the training content generation and environment setup activities. This approach improved the accuracy of the training setup; decreased the setup time and cost; and made repeated training possible for a large number of participants. The framework was evaluated from several perspectives to demonstrate that CyTrONE meets the above objectives. The design requirements were identified as its appropriateness for the target audience (the teachers and students in the case of e-learning systems) according to their knowledge and ability levels; the content according to the development of the skills aimed at; using hands-on activities for practical abilities to deal with later real-life incidents; large audience reach for effectiveness and significant impact; cybersecurity readiness; and a benefit/cost ratio for sustainability. Both the functionality and performance of the model were found to be good.

A trustworthiness model was proposed by Miguel, Caballé, Xhafa, and Prieto (2014) for the design of secure learning assessment for e-learning collaborative groups. The current frameworks have many limitations and vulnerabilities to certain attacks remain. The authors investigated information security requirements in online assessment, (e-assessment), for collaborative e-learning contexts. The model provided guidelines for this purpose. For the assessment of the model, a combination of manual and automatic methods was used. Extracting and structuring LMS data is a costly process for collecting students' data. Hence, a parallel processing approach has been proposed.

Aimed to analyse the control of security and privacy in e-learning systems, Husain and Budiyantara (2020) using the theory of planned behaviour (TPB), attitude and behavioural intention factors that support the university students' e-Learning uses in Indonesia. The causality with questionnaires was used as instruments to collect data from 80 college students. The control of security and privacy was found to significantly influence the attitude and behavioural intention and its implication to the e-Learning users. Attitude and behavioural intention were intervening variables in the effect of the control of security and privacy on eLearning users.

The benefit-cost aspect of e-learning systems security

The Mean Failure Cost (MFC) is a combination of many linear models quantifying the security threats considering the stakeholders, security requirements, architectural components and threats. A quantitative cyber security model of Rjaibi and Rabai (2017) monetised the system's security in terms of cost lost due to security failure. This measure was extended to a security risk management model for very large systems using rigorous and quantifiable analysis of financial returns. A case study of a standard e-learning system was used to validate the model. The conglomeration of linear models used by the author was: MFC = ST ◦ DP ◦ IM ◦ PT, where MFC is the mean failure cost, ST is the stakes matrix (a matrix of a list of stakeholders), DP is the dependency matrix to be filled by the system architects, IM is the impact matrix and PT is the threat vector(each row to be filled by the security team). The case study showed the administrator of the e-learning system ($643 per hour) as the biggest loser, followed by the teacher ($455 per hour). This means, if adequate cyber security arrangements are not made, it will lead to big losses to not only the system administrator but also to the teacher.

Conclusions

The complexity of e-learning systems and their dependence on the internet make them vulnerable to cyber security threats. Especially, as e-learning became the new normal due to the impact of the covid pandemic, this risk still exists and increasing. Despite all the advantages of e-learning, since it uses the internet, e-learning systems are prone to cyberattacks. This review aimed to evaluate some of the available literature on the issues related to e-learning systems.

A search of Google Scholar setting the period as 2014 to 2021, yielded 18 papers for this review. The identified papers were discussed in various sections.

The review informed about the types of cyber-attacks on e-learning systems, solutions to the challenges of cyber security, models and frameworks of cyber-attacks and security issues and the benefit-cost aspect.

The method of relying on Google Scholar rather than databases may have limited the availability of papers. Limiting the period of publication to 2014 to 2021 further reduced the possibility of selecting several papers. However, this was necessary to limit the length of the paper as desired.

References

Alexei, L. A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research, 10*(3), 128-133. Retrieved November 17, 2021, from https://www.researchgate.net/profile/Arina-Alexei/publication/350354392_Cyber_Security_Threat_Analysis_In_Higher_Education_

Institutions_As_A_Result_Of_Distance_Learning/links/6076d5a173e0d20986e0ae86/Cyber-Security-Threat-Analysis-In-Higher-Education-Inst

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and information technologies, 25*(6), 5261-5280. doi:10.1007/s10639-020-10219-y

Alshammari, M., Anane, R., & Hendley, R. J. (2015). The impact of learning style adaptivity in teaching computer security. *Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education, ITICSE '15, 4-8 July 2015, Vilnius, Lithuania* (pp. 135-140). ACM. doi:10.1145/2729094.2742614

Anghel, M., & Pereteanu, G. C. (2020). Cyber Security Approaches in E-Learning. *14th International Technology, Education and Development Conference (INTED2020) Proceedings, 2-4 March, 2020, Valencia, Spain* (pp. 4820-4825). IATED. doi:10.21125/inted.2020.1323

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management, 3*(1), 180-207. Retrieved November 17, 2021, from https://www.researchgate.net/profile/Yair-Levy-3/publication/279801674_Online_Journal_of_Applied_Knowledge_Management_A_Publication_of_the_International_Institute_for_Applied_Knowledge_Management_Examining_users'_personal_information_sharing_awareness_hab

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. *Proceedings of ICERI2014 Conference* (pp. 728-734). IATED. Retrieved November 15, 2021 from https://oro.open.ac.uk/59105/3/59105.pdf

Beuran, R., Pham, C., Tang, D., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2017). Cytrone: An integrated cybersecurity training framework. *n Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)* (pp. 157-166). SCITEPRESS. doi:10.5220/0006206401570166

Cvitić, I., Peraković, D., Periša, M., & Jurcut, A. D. (2021). Methodology for detecting cyber intrusions in e-learning systems during COVID-19 pandemic. *Mobile networks and applications*(June), 1-12. doi:10.1007/s11036-021-01789-3

Durairaj, M. A. (2015). A study on security issues in cloud based e-learning. *Indian Journal of Science and Technology, 8*(8), 757-765. Retrieved November 18, 2021, from https://www.researchgate.net/profile/A-Manimaran/publication/276145699_A_Study_on_Security_Issues_in_Cloud_Based_E-Learning/links/5551707e08ae956a5d25f5f6/A-Study-on-Security-Issues-in-Cloud-Based-E-Learning.pdf

eM Elsawy, A., & Ahmed, O. (2019). E-Learning using the Blackboard system in Light of the Quality of Education and Cyber security. *International Journal of Current Engineering and Technology, 9*(1), 49-54. Retrieved November 15, 2021, from https://asbc.qu.edu.sa/files/shares/%D8%A7%D9%84%D8%A8%D8%AD%D8%AB.pdf

Farid, S., Ahmad, R., Alam, M., Akbar, A., & Chang, V. (2018). A sustainable quality assessment model for the information delivery in E-learning systems. *Information Discovery and Delivery, 46*(1), 1-25. doi:10.1108/IDD-11-2016-0047

Husain, T., & Budiyantara, A. (2020). Analysis of Control Security and Privacy Based on e-Learning Users. *SAR Journal, 3*(2), 51-58. doi:10.18421/SAR32-01

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management system. *8th International Symposium on Digital Forensics and Security (ISDFS), 1-2 June 2020, Beirut, Lebanon* (pp. 1-5). IEEE. doi:10.1109/ISDFS49300.2020.9116415

Kausar, S., Huahu, X., Ullah, A., Wenhao, Z., & Shabir, M. Y. (2020). Fog-assisted secure data exchange for examination and testing in E-learning system. *Mobile Networks and Applications*, 1-17. doi:10.1007/s11036-019-01429-x

Miguel, J., Caballé, S., Xhafa, F., & Prieto, J. (2014). Security in online learning assessment towards an effective trustworthiness approach to support E-learning teams. *28th International Conference on Advanced Information Networking and Applications, 13-16 May 2014, Victoria, BC, Canada* (pp. 123-130). IEEE. doi:10.1109/AINA.2014.106

Nguyen, T. T., & Reddi, V. J. (2019). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*(November), 1-17. doi:10.1109/TNNLS.2021.3121870

Rjaibi, N., & Rabai, L. B. (2017). Maximizing Security Management Performance and Decisions with the MFC Cyber Security Model: e-learning case study. *EAI Endorsed Transactions on e-Learning, 4*(15), 1-12. doi:10.4108/eai.29-11-2017.153389

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on Internet usage and cybersecurity awareness in students. *4th Annual Conference on Privacy, Security and Trust (PST), 12-14 December 2016, Auckland, New Zealand* (pp. 223-228). IEEE. doi:10.1109/PST.2016.7906931