SECURITY UPDATES FOR ENHANCEMENT ON TRUST AND CONFIDENCE IN E-LEARNING SYSTEMS

Nuno S. Silva, Isabel Alvarez

Universidade Lusiada de Lisboa (Portugal), COMEGI / ISTEC (Portugal)

nsas@lis.ulusiada.pt; alvarez@edu.ulusiada.pt

ABSTRACT

The COVID-19 pandemic situation emphasized the need for a strategic response to change educational context, with Governments and educational institutions intending to use this vision and e-learning. This environment is noticeable at three main levels: micro (e.g. the relationship between lecturers and students); meso (e.g. the existing electronic universities' projects); and macro (worldwide governmental actions). Moreover, e-learning, with the utilisation of ICT, causes universities to think globally (competitiveness) and internationally (collaboration). However, to presume that technology by itself entails education is unrealistic and condemns any e-learning paradigm, because novel technologies impose substantial security issues. This work intends to plan a risk mitigation regarding e-learning security implementation. The confidence in the availability, and non-repudiation, should be combined with the aim of reaching information security requirements for e-learning systems as a precondition for enhanced user acceptance. Trust is also essential to get the better of privacy concerns.

INTRODUCTION

In e-learning, attention should be paid to security elements such as availability, integrity and confidentiality to avoid any security breaches that may harm educational institutions (Okafor, Oparah & Okwudili, 2018). The credibility of online learning and the privacy of students and staff need to the considered. Any e-learning system is supported by the Internet which is insecure and which opens a door to any software attack. However not much has been done to avoid this situation. To guarantee a safer e-learning environment and avoid these threats, security should be a priority.

E-learning promotes the existence of a strategic response to a novel educational context, which is emphasised by the COVID-19 pandemic (Almaiah, Al-Khasawneh, and Althunibat, 2020). Governments and educational institutions intend to use this vision. The use of Information and Communication Technologies (ICT) mean large changes to the way lecturers, students and universities use to work. However, to presume that technology by itself entails education is unrealistic and condemns any e-learning paradigm, as instructional quality, privacy, and mobility need substantial security issues with the use of technology. Moreover, E-learning causes universities to think globally (competitiveness) and internationally (collaboration), although these distributed knowledge networks may cause several ethical and cultural dilemmas.

This work suggests a risk mitigation plan regarding e-learning security implementation; we propose the exploration of four levels: Technological Infrastructures and Services, Knowledge/Content Management, Computer Mediated Communication, and Value-added.

To mitigate web attacks on e-learning platforms, Wani & Khan (2016) refer the critical security issues that an e-learning platform must address and a methodology of development that should incorporate security components at the design phase to avoid these threats.

DIMENSIONS OF E-LEARNING

Overview

The e-learning literature is vast. Several authors refer that this form of learning currently depends on networks and computers but will likely evolve into systems consisting of a variety of channels. It is essential to understand the global perspectives of e-learning intervention, as, for example, it refers to the complex connections between strategies, design, and technologies, which encompass the following components of policymaking: strategic planning and vision; curriculum and content; use of the internet and acceptable use policies; quality assurance and accreditation; conductivity, infrastructure, and networks; professional development; intellectual property and copyright; cost, finance, and partnerships; factors such as leadership, culture, structure, design and technology, as well as delivery management. In spite of this, it is suggested that four levels are explored: Technological Infrastructures and Services, Knowledge/Content Management, Computer Mediated Communication, and Value-added.

Technical Infrastructure and services

As for technological infrastructure and services, the e-learning implementation at university settings is a complex task, which starts with a strategy for developing the basic technical infrastructure. According to Blinco, Mason, McLean & Wilson (2004, p. 2), this “infrastructure often describes a bottom layer of an architectural description or diagram, indicating network hardware components, communication processes, services and protocols”. Throughout this assumption it is vital to shed some light over what are the issues in a "bottom layer". First of all, it needs a comprehensive functional and technical analysis to determine how technology should be applied, where equity of access is an important factor, and what security levels are to be implemented (e.g. firewalls).

Although the internet is the basic network infrastructure for e-learning it is, however, necessary to consider components at local networks, as well as personal tools and equipment that make learning activity possible. Management systems assume particular importance on this assumption as the e-learning evolution comprise four general categories of technological systems: Learning Management Systems, Managed Learning Environment, Learning Content Management Systems and Virtual Learning Environments. Furthermore, several other dilemmas may emerge asking for a global open source solution (like, for instance, Google).

Knowledge/content management

In what concerns knowledge/content management, e-learning also includes content over technology, or, following Hartley (2014) educational content is more important than technologies. This assumption leads us to explore content related issues in e-learning implementation, and thereby the need for a new conception of security understanding.

It is discussed and argued that a clear perception of the boundaries of knowledge versus content is required, since these two concepts also influence pedagogical strategies in e-learning practices. If on

one side knowledge is dependent on conceptual skills and cognitive abilities, on the other content refers to the encoded "unprocessed material" which achieves the objectives that the content creator has set for it.

In traditional learning approaches (behaviourism, cognitivism and constructivism), and aiming that learners master knowledge through drill and practice, content is categorized according to its encoded meaning; it should be measured by the fulfilment of the end goals as being highly interactive and add value. In an e-learning implementation both these two statements, due to the interactivity potential of computer-mediated communications, are subject to transformation in what concerns the knowledge/content creation.

Computer-mediated communication

In computer-mediated communication, the interactivity is a key characteristic of e-learning within the communication processes to be analysed. Computer Mediated Communication (CMC) should be explored in regard to one additional layer to understand the e-learning implementation. According to Zhang (2004), CMC transforms classrooms to make learning a more interactive, diverse and enjoyable experience. This can be through online interactive classrooms, interactive group discussions and tutor/student sessions, or empowering students/teachers' interactions by designing more flexible and intuitive interfaces. In this educational paradigm, learning "with" interactive technologies establishes a certain intellectual affiliation between students and technologies. Instead of using technologies to guide students through prearranged interactions, students may use technologies that function as "the mindful engagement of students". The social presence created in an online community was a strong predictor of satisfaction in CMC, building learning communities. However, how can CMC support satisfactory socio-emotional and relational communication compared with face-to face communication. How can this evolution of learning through technologies replace teaching as essentially a human relation, face to face relationships, and social isolation in front of a computer screen. In spite of robot deployed as classroom teachers, there is a risk that children would lose emotional security (Sharkey, 2016).

We need to implement a balanced approach to avoid ignoring technology tools or fixating too much on technology for e-learning. The videoconferencing is considered as the CMC tool that is the closest to face-to-face communication, enabling high levels of interaction and facilitating personal feelings (e.g. social presence and perceived privacy), while security breaches are usually out of risk analysis and its related streaming media services, like the recorded classroom lectures or video-broadcast seem to hold an important value.

However, following May et al. (2012) using a CMC tool alone, participants claim that their activities are not fully controlled as when learning in a traditional face-to-face situation. In what concerns tracking technologies, if users are informed in anticipation of any tracking process being used in the platform that they are accessing, having the possibility to give their approval for this tracking process to take place, then they should not consider these technologies as a threat. It is assumed that in a collaborative learning situation where intense interactions and exchanges of both personal and collaborative data take place, there should be a specifically designed environment to guarantee the protection of the learner's privacy.

Value added

Value added emerged as an important approach to e-learning (for instance related to time investment costs, content valuable functionality, and use of streaming media services). So, in this scenario, it is possible to understand that e-learning adds value to the learning experience, but it is not clear what issues mean “value of e-learning” (financial notion on the measure of benefit), or “e-learning values” (ethically and culturally sensitive to meanings that may vary according to context). Therefore, it is important to explore if it justifies a “top layer” to understand the e-learning implementation.

In late 2019 a novel worldwide health situation unexpectedly emerged: the sarscov2, a new type of coronavirus was identified (WHO, 2020). Due to the pandemic restrictions, e-learning was enforced as the only way to proceed with learning. Based on this experience, most people are looking at this opportunity to introduce and implement innovative alterations in the education system (Bird & Bhardwaj, 2020). Researchers should take this opportunity to understand and explore the crisis implications in terms of learning, evaluate the impacts and the financial consequences of this pandemic and develop models of policy interventions (Brammer & Clark, 2020). In the outcome, it can be learned from this pandemic experience, that they could adjust to different environments and situations, facing and solving new difficulties and conclude that positive perspectives arose from the quarantines.

From the teacher’s perspective, the increasing use of digital platforms like the interactive meeting tools – Zoom, Google Meet, Microsoft Teams or Cisco Webex – was seen as the best way to continue with learning. After this very interesting pandemic experience, some advantages can be seen in the use of online learning, like the flexibility of time and place, inducing to reflexive innovations in the practices and schedules of academic structure (Brammer & Clark, 2020). However, the impact of COVID-19 in education cannot yet be fully understood (eLearning Inside, 2021; Zhao & Watterston, 2021). Moreover, in what concerns security breaches of this impact needs a research focus that is not yet developed.

Xie (2020) refers some of the threats of online education: network instability and technological constraints; lack of a sense of belonging and connectedness; presence of distractions. It can be considered that this pandemic scenario provided a chance to improve their information literacy and security awareness. Having to learn how to use new tools and software that they were not acquainted before, was indeed a “learning opportunity” leading to thoughtful decisions in the future of e-learning.

E-learning and Cloud computing

From an educational point of view, and acknowledging that cloud computing might provide unlimited resources for storage capacity and data processing, universities will become a key element in future security systems. A variety of services through pay per use and fee-based infrastructure with value added infrastructure will be offered to the users of cloud computing (Arora & Sharma, 2013), as this innovative technology delivers computing resources through globalised circulation networks.

The introduction of cloud computing in the educational systems acknowledges the purpose of increasing scalability, flexibility and availability at the application level (Popel & Shyshkina, 2019).

In addition, cloud-based LCMS (Learning Content management Systems) centralizes content management, while providing in-depth performance metrics, ensuring resolution in time to execute developments, support, updates and fixes.

Cloud computing increasing interest has implications for security, privacy, and trust. Compliance with European GDPR requirements is a critical requirement. COVID-19 caused the criticality of technology to increase the use of platforms such as VPN, video conferencing tools, and home computer equipment. This implies that the SLAs associated with these environments must be improved. Even so, governance of emerging technologies is critical to undertake advanced measures to protect the most security-sensitive information stored (Rawtani, 2012). The confidence in the availability, and non-repudiation, should be combined with the aim of reaching information security requirements for e-learning systems as a precondition for enhanced user acceptance (Moneo, et al. 2016; Weippl, 2005). In addition, the diversity of mobile devices and their security protection measures are varied in accordance with the operating system (May Iksal & Usener, 2017), and biometric web authentication can be useful for proper identification of learners (Goyal & Krishnamurthi, 2019).

In spite of the foreseen important short and long-term benefits that cloud computing will bring to a scholarly environment, being an emergent technology, serious perils and ethical challenges may occur and need to be considered. The increasing interest by policymakers and regulatory authorities in cloud computing is due to the possible implications in security, privacy and trust (Rand Europe, 2011). Although privacy may yet be in opposite laws and debates (EDRI, 2021; Salter, 2019), while not only the legality but also the morality is important in cyber security (Hamburg & Grosch, 2017).

Indeed, the governance of emerging technologies, whose menace can merely be lessened, is critical to undertake advanced measures to protect the most security-sensitive information stored (Rawtani, 2012). A responsible management of personal data becomes a key issue to ensure trust in cloud-based services adoption and encouraging users to explore them (Pearson, 2013).

Data security covers main areas like encryption, and password security. It should be considered to the appropriate balance between law practices and protecting confidential data in cloud-based storage.

It is relevant to report problems for instance in SSO (Single-Sign-On) synchronisation, content synchronisation, trust of passwords (external security), and the unexpected software updates; some novel functionalities of cloud computing desperate users due to the lack of usability!

Furthermore it can be merged with high compromise of top management in security strategies which made part of ISO/IEC 31000 and ISO/IEC 27005 risk assessment standards.

Trust and confidence

Concerning trust management, various issues should be taken in consideration like privacy of users (learners and teachers) including issues related to grading, competency, and personal information (Wani & Khan. (2016). Itani, et al. (2014) for instance suggest that the minimum service metrics (reliability, availability, performance and security) for cloud service provider based on SLAs (Service Level Agreement) which, if fails, will affect reputation and trust.

May & George (2011) suggest that trust is part of the solution. Trust is confidence on someone's competence and commitment to achieve a goal and crucial to build and assist relevant interactions in learners collaboration.

Trust is also essential to get the better of privacy concerns on using technological solutions and not only to keep users safe from any threats. In practice, privacy and trust are circularly related, as privacy is a natural concern at the same time that trust is an essential factor in the learning environment. In fact, in a closed learning environment, where all learning services are provided internally (e.g. from a university or a trusted source) students can have higher confidence that their personal data and

learning tasks such as working collaboratively will be treated properly On the other hand, in an open learning environment with unknown providers such as private or external learning service providers, privacy concerns are higher and the trust level of learners will be influenced by the perceived privacy offered by those providers; these privacy issues concern learning technology providers, learning service and content providers and the participants as well, with the crucial tasks for learning service and content providers being to secure learning environment and storage of learner data. As for the participants, they are mainly concerned with the trust assessment of the learning environments they are using, and with the protection of their sensitive personal data; also understanding the security issues in the learning situations helps them to avoid security threats as well as to improve protection of both themselves and their learning environments. Security and privacy levels differ according to the various learning environments and depend on the types of learning activities being done by the participants. From May (2011), the following issues concerning learning technology: personal data protection, anonymous use of learning services, address and location privacy, single sign-on, seamless access to learning resources, authenticity of learning resources (Las), digital rights management, legislation and awareness raising require different protection provisions.

Presently students have an increasing understanding and knowledge of information systems (IS) and information technology (IT) issues. To build digital trust and to assist the students’ needs all the learning strategies devised by course providers must be linked with IS/IT strategies whether now or in the future (Bandara, Ioras, & Maher, 2014). In terms of usability, security and protection of their personal information, digital natives and immigrants will share expectations of their e-learning systems; this could refer, for instance, the inclusion of students’ details associated with payments for course fees and other products, done in a secure way. The important intellectual property connected with research and other academic material existent in the UK Universities could attract cyber-criminals and researchers will expect that their important work and sensitive information is properly and securely stored, with no risk of theft or misuse. Institutions should perform a cyber security risk assessment and determine best arrangements for technology, people and processes.

To plan a risk mitigation regarding e-learning security implementation

To plan a risk mitigation regarding e-learning security implementation, there are several issues to be considered: Internet bandwidth must be recognised as fundamental, alongside issues like speed, accessibility, cost and reliability; wireless networks and mobile computing for students is a key benefit because it avoids the need for physical presence; videoconference implementation enabling online-only teaching (e.g. Microsoft Teams, Zoom, Google Meet or Cisco Webex); and the cyberthreats of online learning platforms, as for example Moodle e-learning environment added value related to access, privacy and security, since lecturers can make content available only for students who must take the inherent access rights for course units. Concerning ethical assessment of the idea of robot teachers, Sharkey (2016) report the relevance of issues including privacy, control, and accountability.

It is also typical to report problems at meso level, for instance in SSO (Single-Sign-On) synchronization, content synchronisation, trust of passwords (PKI and external security) (Miguel, Caballé, & Xhafa, 2017), and the unexpected software updates; also a self-service integrated system allows printing, photocopying and scanning of content, where security is based on password request (security breaches in networked printing systems). Another aspect of security is the existing backup policy. Moreover, it is important to mitigate the risk rating of all external assets, such as web applications, IP addresses, and marketing sites. For example, a Moodle penetration testing when performed can reveal important issues for risk monitorization. This study intends to merge a new security sensitivity

metric for such variables. It includes security updates and best practices that effectively minimize risks related to using cloud computing.

Schinagl, Schoon, & Paans (2015) developed a measurement method to assess the effectiveness of the protection provided by a SOC (Security Operations Centre), which is responsible for the activities related to security monitoring as well as to address situations that jeopardize the confidentiality, integrity and availability of technological services and electronic information that the university administers. The SOC staff to cover the following functions: Manager - the group leader that can assume any role while overseeing general security systems and procedures; Analyst - Analysts compile and analyse data, either from a period of time or after a breach; Investigator - Once a violation occurs, the investigator finds out what happened and why, working closely with the responder; Responder - Tasks that come with responding to a security breach; Auditor - Current and future legislation comes with compliance mandates. This feature can keep up to date these requirements and ensures that the organization meets them.

According to NIST (2012), a computer security incident is the imminent violation or threat to an information security policy violation (acceptable use policies or standard security practices).

Given such a reality, it is important to refer to two levels of arguments concerning e-learning security updates:

- as a strategy - organisational change addressing security issues;
- as a tool - socio-technical dimension of security breaches (password security level and data protection).

Therefore, in order to minimise potential failures, it is crucial to involve all stakeholders to have security awareness and security sensitivity as a prerequisite for trust and confidence in national and international successful e-learning implementation.

The mobile services available anywhere around the world, has been impacted by the continuous growth in the numbers of smart devices and related connectivity loads. Authentication is in fact, in such a connected globe, in the first place, the enabler keeping the transmitted data secure (Alomar, Alsaleh, & Alarifi, 2017).

Actually, there are three factor groups available to connect an individual with the established credentials (Harini, & Padmanabhan, 2013):

1. Knowledge factor—something that is only knwn to the user, such as a password or, simply, a “secret”;
2. Ownership factor—something the user has, such as cards, smartphones, or other tokens;
3. Biometric factor—something the user is: it could be biometric data or a behaviour pattern.

As suggested by Mohsin et al. (2017), to provide a better level of security and to ease continuous protection of computing devices together with other critical services from unauthorized access by using more than two categories of credentials, the Multi-Factor Authentication (MFA) is proposed.

Confidentiality, Integrity, and Availability, are the basis of all security programs and security in computing concentrates on tools, processes and methods to design, develop and implement reliable systems (Asmaa, & Najib, 2016). Examining Moodle, one of the most used and popular open-source

e-learning systems - a system needs to implement security services such as authentication, encryption, access control, managing users and their permissions. However, several vulnerabilities are historically reported (CVE, 2021), with statistics put in the top for Moodle both "Gain information" (allows remote attackers to obtain sensitive information), and XSS (an attacker to compromise the interactions that users have).

To conclude, a secure e-learning platform should include all the types of security producing transparent processes both to the teacher and student. It is assumed that in the future the concept of m-learning will come in new electronic learning features but, in parallel, new risks will also occur.

Information security and privacy such as confidentiality, integrity, authentication, and non-repudiation, is no longer only a highly desired feature but it is now an essential legal required condition of any information system, with e-learning being not an exception (Wani, & Khan, 2016). Any e-learning platform is web based and therefore is prone to diverse attacks, such as brute force attacks, XSS (or Cross Side Scripting), direct SQL code injection, remote SQL injection using a virus/trojan file, SQL injection in the site address CURL SQL injection), web indexing, session predictions, password cracking, etc. At present, not many e-learning systems have proper security design and privacy characteristics integrated into the e-learning development and implementation process. Consequently, such systems can cause serious issues in maintenance of learning objects, authentication in student/teacher registration, scheduling of events, protection of user profiles, conduct of remote assessments and examinations, and certification award. Vulnerabilities can be accidentally and intentionally introduced throughout the software development life cycle during requirements definition, design, implementation, deployment and maintenance and e-learning systems are vulnerable to a number of threats: serious security threats include software attacks (viruses, worms, macros, denial of service), espionage, acts of theft (illegal equipment or information) and intellectual property (piracy, copyright, infringement) (Bandara, Ioras, & Maher, 2014).

The learner data is normally used to enhance the learner's security position by continuous delivery of important information and accommodating security mechanisms (Milošević, & Milošević, 2016). From the list of presented protection measures, the most urgent ones are those related to potential security and privacy threats and protection of personal data, while the least urgent (but still relevant) is the anonymous use of learning resources. An e-learning system being a web-based system and must be protected from any computer threats to ensure the tranquillity of the users when using it, with or without online webcams.

This study has also investigated the security benefits and increased threats of shifting from traditional monolithic system to modern e-learning ecosystem or cloud-based system, also examining loss or theft of mobile device, unauthorised access, attack on m-learning system and denial of service.

Finally, Universities have to carry out actions and create resources that promote information security at micro level (MetaRed, 2021), and for that, the recommended example is the Cybersecurity Awareness Kit developed for Ibero-American Universities as a collaborative project with Spanish Cybersecurity Institute (INCIBE).

Therefore, there are dilemmas to conceive e-learning goal from the macro level, namely if it enlarges the scope of traditional university. For the purpose of innovation and change in the university role it may enhance the traditional forms of university teaching and administration (hybridisation), but the user's perspective early in the implementation process should be taken in a responsible way, namely balancing the push/pull action (whole strategy and involvement) and enabling ethical perspectives on security enhancements.

CONCLUSION

COVID-19 caused the criticality of technology by increasing the use of e-learning. With the world moving towards being increasingly dependent on computers and automation, one of the main challenges in the current decade has been to build secure applications, systems, and networks. Therefore, in order to minimise potential failures, it is crucial to involve all stakeholders to have security awareness and security sensitivity as a prerequisite for trust and confidence in national and international successful e-learning implementation. Trust is confidence on someone's commitment to achieve a security goal.

Online learning is built on trust, information exchange, and discussion. However, due to the unexpected problem of the pandemic COVID-19, online learning providers had and still have to face a difficult balance, trying to provide sufficient security to protect online learning resources while not inhibiting the appropriate use of these resources. Our study focused on the suggestion of development and implementation of an improved e-learner model that supports monitoring of user behaviour related to information security. It is important to plan a risk mitigation in e-learning security.

KEYWORDS: e-learning, COVID-19, Security, Trust, Confidence.

REFERENCES

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*, 1(20). https://doi.org/10.1007/s10639-020-10219-y

Alomar, N.; Alsaleh, M.; Alarifi, A. (2017). Social authentication applications, attacks, defense strategies and future research directions: A systematic review. IEEE Commun. Surv. Tutor., https://doi.org/10.1109/COMST.2017.2651741

Arora, A. S., & Sharma, M. K. (2013). A proposed architecture of cloud computing based e-learning system. International Journal of Computer Science, & Network Security, 13(8), 31-34.

Asmaa, K., & Najib, E. (2016), E-learning Systems Risks and their Security. International Journal of Computer Science and Information Security (IJCSIS), 14(7).

Bandara, I.; Ioras, F. and Maher, K. (2014). Cyber Security Concerns in E-learning Education. In: Proceedings of ICERI2014 Conference, IATED, 0728-0734.

Bird, C., & Bhardwaj, H. (2020). From Crisis to Opportunity: Rethinking Education in the Wake of COVID-19, Child, & Youth Services, 41, 228-230.

Blinco, K., Mason, J., McLean, N., & Wilson, S. (2004). Trends and issues in e-learning infrastructure development. White Paper, ALT-I-LAB, California. Retrieved from http://www.jisc.ac.uk/uploaded_documents/Altilab04-infrastructureV2.pdf

Brammer, S., & Clark, T. (2020). COVID-19 and management education: Reflections on challenges, opportunities, and potential futures. British Journal of Management, 31, 453-456.

CVE (2021). Moodle: Vulnerability Statistics. Retrieved from https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105

EDRI. (2021). A victory for us all: European Court of Justice makes landmark ruling to invalidate the Privacy Shield. European Digital Rights Ass. Retrieved from https://edri.org/our-work/a-victory-for-us-all-european-court-of-justice-makes-landmark-ruling-to-invalidate-the-privacy-shield

E-learning Inside (2021). How COVID-19 Has Changed Education and How to Adapt. E-learning Inside, 08 January. Retrieved from https://news.elearninginside.com/how-covid-19-has-changed-education-and-how-to-adapt/ (25/03/2021)

Goyal, M., & Krishnamurthi, R. (2019). An Enhanced Integration of Voice-, Face-, and Signature-Based Authentication System for Learning Content Management System. In Kumar, A. (Ed.), Biometric Authentication in Online Learning Environments (pp. 70-96). IGI Global. http://doi:10.4018/978-1-5225-7724-9.ch004

Hamburg, I., & Grosch, K. R. (2017). Ethical Aspects in Cyber Security. Archives of Business Research, 5(10), 199-206.

Harini, N.; Padmanabhan, T.R. (2013). 2CAuth: A new two factor authentication scheme using QR-code. Int. J. Eng. Technol. 2013, 5, 1087–1094.

Hartley, R. (2014). Conceptualising and supporting the learning process by conceptual mapping. Smart Learn. Environ. 1(7). https://doi.org/10.1186/s40561-014-0007-2

Itani, W., Ghali, C., Kayssi, A., Chehab, A. (2014) Reputation as a Service: A System for Ranking Service Providers in Cloud Systems. In: Nepal S., Pathan M. (eds) Security, Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38586-5_13

May, M., & George, S. (2011). Using students tracking data in E-learning: Are we always aware of security and privacy concerns 2011. IEEE 3rd International Conference on Communication Software and Networks: ICCSN 2011.

May, Madeth, Fesakis, Georgios, Dimitracopoulou, Angelique, & George, Sébastien. (2012). A Study on User's Perception in E-learning Security and Privacy Issues. Proceedings of the 12th IEEE International Conference on Advanced Learning Technologies, ICALT 2012. 88-89. https://doi.org/10.1109/ICALT.2012.145.

May, M., Iksal, S., Usener, C. A. (2017). The side effect of learning analytics: An empirical study on e-learning technologies and user privacy. In Costagliola, G., Uhomoibhi, J., Zvacek, S., McLaren, B. M. (Eds.), *Computers supported education* (Vol. 739, pp. 279–295).

Metared (2021). Kit de concienciación en ciberseguridad - Edición IES iberoamericanas. Retrieved from https://www.metared.org/global/kit-concienciacion-cyber.html

Miguel, J., Caballé, S., & Xhafa, F. (2017). Intelligent Data Analysis for e-learning: Enhancing Security and Trustworthiness in Online Learning Systems. San Diego: Academic Press.

Milošević, M., Milošević, D. (2016). Defining the e-learner’s security profile: Towards awareness improvement. Sādhanā 41, 317–326. https://doi.org/10.1007/s12046-016-0478-7

Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. (2017). Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39.

Moneo, J. M., Caballé, S., Xhafa, F., Prieto-Blázquez, J., & Barolli, L. (2016). A methodological approach for **trust**worthiness assessment and prediction in mobile online collaborative learning. Computer Standards, & Interfaces, 44, 122-136. https://doi.org/10.1016/j.csi.2015.04.008

NIST (2012). Computer Security Incident Handling Guide NIST. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Okafor, N. U., Oparah, C. C., & Okwudili, U.M. (2018). Security and Privacy in E-learning Education. Journal of Arts, Physical and Social Sciences, Federal Polytechnic Nekede, Owerri 1(1): 40-43.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In S. Pearson, & G. Yee (Eds.), Privacy and Security for Cloud Computing (pp. 3-43). London: Computer Communications and Networks. Springer-Verlag.

Popel, M., & Shyshkina, M. (2019). The areas of educational studies of the cloud-based learning systems. Educational Dimension, 53(1), 60-79.

Rand Europe. (2011). The cloud: Understanding the security, privacy and trust challenges (technical report). RAND. Retrieved from http://www.rand.org.

Rawtani, M. R. (2012). Achieving knowledge management through cloud computing. In V. Prakash et al. (Eds.), *8th Convention PLANNER-2012* (pp. 387-394). Gangtok: Sikkim University.

Salter, J. (2019). Office 365 declared illegal in German schools due to privacy risks. Arstechnica. Retrieved from https://arstechnica.com/information-technology/2019/07/germany-threatens-to-break-up-with-microsoft-office-again/

Schinagl, S., Schoon, K., & Paans, R. (2015). "A Framework for Designing a Security Operations Centre (SOC)," 2015 48th Hawaii International Conference on System Sciences, 2015, pp. 2253-2262, doi: 10.1109/HICSS.2015.270.

Sharkey, A. J. C. (2016). Should we welcome robot teachers? Ethics and Information Technology, 18(4), 283–297. https://doi.org/10.1007/s10676-016-9387-z

Wani, F. H., & Khan, R. A. (2016). A Study of Security and Privacy Issues in E-learning Platforms. Two day national seminar on Electronic Devices, System and Information Security (SEEDS-2016) held by Department of Electronics, & IT, University of Kashmir from 18-19 March, 2016.

Weippl, E.R., 2005. Security in e-learning, New York, NY: Springer.

World Health Organization (WHO). (2020). Listings of WHO's response to COVID-19. Retrieved from https://www.who.int/news/item/29-06-2020-covidtimeline

Xie, X., Siau, K., Fui-Hoon Nah, F. (2020) COVID-19 pandemic - Online education in the new normal and the next normal. Journal of Information Technology Case an Application Research, 22, 175-187.

Zhang, D. (2004). Can e-learning replace classroom learning? *Communications of the ACM,* 47(5), 75-79.

Zhao, Y., Watterston, J. (2021). The changes we need: Education post COVID-19. Journal of Educational Change, 22, 3–12.