Journal of Information Systems and Informatics
Vol. 5, No. 4, December 2023 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v5i4.583 Published By DRPM-UBD

Cybersecurity Cloud-Based Online Learning: A Literature Review Approach

Vusumuzi Malele[1]

[1]North-West University, Potchefstroom, South Africa
Email: vusi.malele@nwu.ac.za[1]

Abstract

Cloud-based online learning is the electronic learning activity that supports teaching and learning (T&L) that could be done from anywhere and in the world. Some of its benefits are scalability and affordability that could in a decision-making support on the mechanisms of material selection. Cloud computing has been adopted by most universities around the world. In this regard, lecturers and students will use it to facilitate T&L; however, due to concerns of information technology or systems security, cloud-based online learning users are also not immune. In this regard, the users could be affected by different cybersecurity attacks. In this paper, a systematic literature review method was used to sift the different models and solutions used to address the cybersecurity concerns surrounding cloud-based online learning. A brief Likert-scale questionnaire was used to obtained data that could corroborate the systematic literature findings. In this regard, a group of 20 online learning designers were sampled as participants. It was found that the confidentiality, integrity, and availability issues are a concern. This led to issues of security awareness, authentication and blended attacks being issues. In this regard, a cloud-based online learning model is not immune from security issues. In this paper, a conceptual framework as the line-of-defense is proposed as a solution towards having a cybersecure cloud based online learning.

Keywords: Cloud-based learning, online learning, security, blended attacks

1. INTRODUCTION

Education 4.0 has seen to it that online learning such as electronic learning (e-learning), mobile learning (m-learning) and distance learning using technology, among other things have one thing in common, the connection and use of the internet. Most of these online learning education models are implemented and facilitated through a cloud-based learning management system (LMS). The latter is known as the cloud-based online learning [1, 2].

Cloud-based LMS allows educators and learners to access the platform from anywhere and at any time. Cloud based LMS do not require the installation of

hardware or software as everything is provided through cloud computing. For example, all the data is stored in the cloud making it possible Wifi and Bluetooth enable devices to use the cloud based LMS. Cloud-based LMS also allows social, economic, scientific and engineering tools to be embedded on it. For example, Facebook, games, simulations, and virtualization are now part of the cloud based LMS [3]. Cloud-based LMS facilitate cloud-based online learning.

Cloud-based online learning is the modern way of conducting classes that takes place in the cloud connected to the internet. Approximately in every 40–to–60 seconds the internet is affected by cyber-attacks [4]. In 2022, at most 1–in–5 internet users were affected by cyber-crime [4]. There are several security concerns in the cloud-based online computing environment. Several security concerns such as Tenant Security Requirement Manager (TSRM), Lightweight IDS (LIDS) and Remote Advanced Attack Detection (RAAD) exist within software as a service (SaaS) in the cloud computing environment. SaaS is an efficient, flexible, and low-cost security service model.

Due to the increase and popularity of cloud-based learning security arises on data breaches that hackers could try and use to exploit the security vulnerabilities of the cloud [5]. The key cloud security challenges are [6]: (i) Authentication - All unauthorized people have access to the data that a cloud user has saved on the internet; (ii) Access control - To ensure that only authorized users are promoted, the cloud must have appropriate access control policies; and (iii) Policy integration - The cloud must have adequate access control measures in place to guarantee that only approved users are promoted. Cloud-based learning infrastructure also faces the potential vulnerabilities through privacy, and trust issues that might create risk to cloud data [7]. In this regard, cloud based LMS plays a vital role as it helps with managing authorization, identity management, and authentication. Furthermore, network security could also be protected by through firewalls. Furthermore, SaaS security issue talks to the idea that it must provide integrity. confidentiality and availability across all software application [8]. The most important component is user verification, as the administration of passwords might damage security. Access should be granted to the appropriate user according to their roles in an organization. The role of trusted computing platforms in cloud computing and the role of trusted computing in cloud computing.

Cloud based online learning users could be affected by different cybersecurity attacks. Against this backdrop, this paper uses a systematic literature review (SLR) method to sift for different models and solutions that address the cybersecurity concerns surrounding cloud-based online learning. The literature findings were validated using the questionnaire that was distributed to a group of online learning content designers. This paper adopted the IMRAD paper style. In this regard,

despite this introduction, section II briefly discusses the methodology, section III briefly discusses the results and validation. The conclusion is provided section IV.

2. METHODOLOGY

In this paper the SLR method was adopted. Figure 1 illustrates the research strategy that was followed to conduct the SLR. This paper aims to get insight into what studies have been published in the domain of cybersecurity cloud-based online learning and cloud LMS.

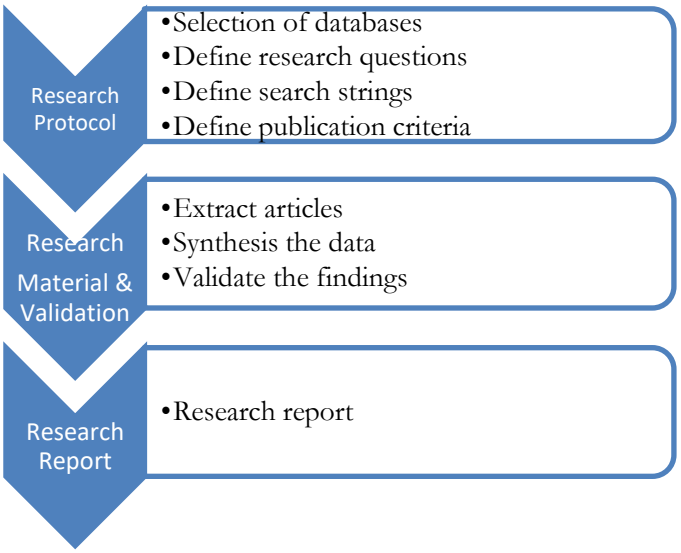

Figure 1. The adopted research strategy for conducting the SLR.

2.1 Research Protocol

Selection of Databases – The literature search process involves querying available literature on cybersecurity cloud-based online learning and LMS. Most computing researchers' work is indexed and stored in the following digital libraries Scopus, Semantic Scholar, Google Scholar, IEEE Xplore, and ACM Digital Library. In this regard, for the purpose of this article only the IEEE Xplore, and ACM Digital Library were consulted.

Define Research Questions – The research questions were guided by the key concerns of general cybersecurity issues and online learning. It was refined through preliminary literature that was conducted on cloud based online learning, which formed the genesis and crux of this paper. For this paper, the following research

questions (RQs) were used as the guide: (i) RQ 1: What are the cybersecurity concerns of cloud based LMS? and (ii) RQ2: What is the cloud-based online learning cybersecurity models that could be effective for implementation in higher education?

Define the Search Protocol – In this paper, the search criterion was set to only focus on English written articles published between 2015 to 2023. The following inclusion search criterion string was used:

1) (Cybersecurity AND Online Learning AND (higher education OR general*))
2) (Cybersecurity AND Cloud-based AND Online Learning AND Models AND (higher education OR general*))
3) (Cybersecurity AND Model AND Cloud-based AND Learning Management Systems AND (higher education OR general*))

To exclude irrelevant articles, the following exclusion criterion (EC) was used to set the boundaries of this SLR method:

1) EC 1 – Publication is not written in English.
2) EC 2 - Publication is not related to cybersecurity cloud computing and LMS issues.
3) EC 3 – Publication that is a duplicate or already retrieved from another database.
4) EC 4 – Full text of the publication is not available.
5) EC 5 – Publication not a peer-reviewed paper.
6) EC 6 – Publication has been before 2015.

2.2 Research Material and Validation

Research Material extraction – the articles were extracted by narrowing down the search criteria based on RQ1 and RQ2. Table 1 provides the details of such extraction. In this regard, the thematic analysis was conducted on the extracted data.

Research Validation – the questionnaire with the themes was sent to 20 randomly selected online designers to determine if they corroborate the themes emanating from the extracted data.

2.3 Research Report

This article forms the research report highlighted in Figure 1. The report results will be presented in the next section.

3. RESULTS AND DISCUSSION

3.1 Search Results

Cybersecurity and privacy in cloud computing has always been a challenge. Different studies have been retrieved from mainly the IEEE Xplore, and ACM Digital Library. These articles point and discuss the general cybersecurity, cybersecurity for online learning, cybersecurity for cloud computing and cybersecurity for LMS. For example, the ACM digital library gave an output of 632,453 from 1951 to 2023; and when filtered to the relevant years (January 2018 to January 2023) it yielded 171,441 articles. While IEEE 951 from 2010 to 2023; and only 8 from 2017 to 2023. The latter was relevant to cybersecurity for cloud based online learning. of the 171,441 articles only 20 closely related to cybersecurity for cloud based online learning.

Figure 2. Thematic issues in cybersecurity cloud based.

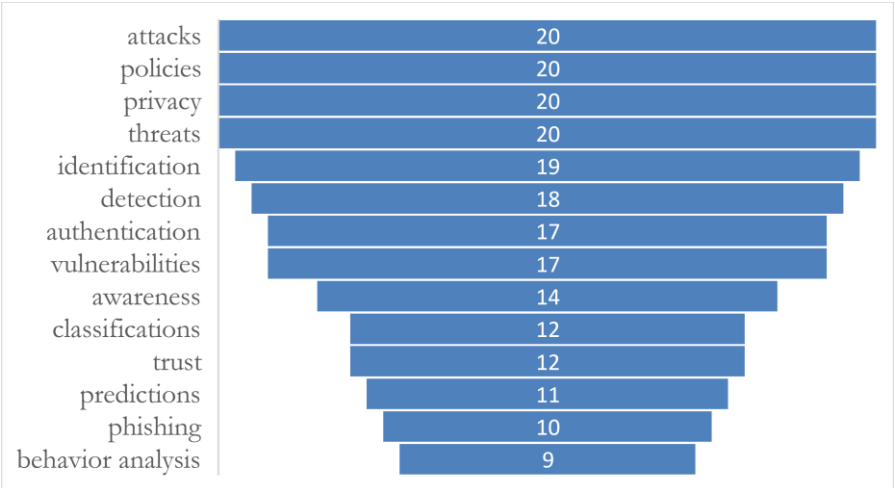

Figure 3. Corroboration by professionals.

Figure 2 illustrates the thematic areas that emerged from analysis of the extracted studies. Thematic areas that still prevalent in cybersecurity cloud-based online learning area: data access (confidentiality), data accuracy (integrity), data accessible to rightful people who need it (availability), privacy paradox, authentication, identification, trust, exploits, vulnerabilities, threats, cybersecurity behavior analysis, cybersecurity awareness, system thinking cybersecurity, information security and cybersecurity policies, and attacks (flooding, blocking, blended) [8-20]. For example, flooding attack creates numerous requests in the form of small messages which block the entire season preventing the cloud-based client (student/lecturer/administrator) from obtaining access. The blocking attack usually is the external person who got permission to access cloud-based online learning material and then temper with material. Furthermore, Figure 2 illustrates thematic areas aligned to intelligent cybersecurity systems such as classification, blockchain, neural-networks, social networks, framework and model development, anomaly detection, phishing detection, buffer-overflow, and many more [21-27]. The above findings led to a thinking of conducting a brief questionnaire survey with a sample of 20 online learning designers that work in the cloud based online learning environment. The aim of the brief survey was to determine or corroborate whether the literature extracted thematic areas (as illustrated in Figure 2) align to their experiences. Figure 3 illustrates the findings of the survey, showing that all the professionals agreed that attacks, policies, privacy and treats are key cybersecurity issues affecting their day-to-day operations.

3.2 Recommendation

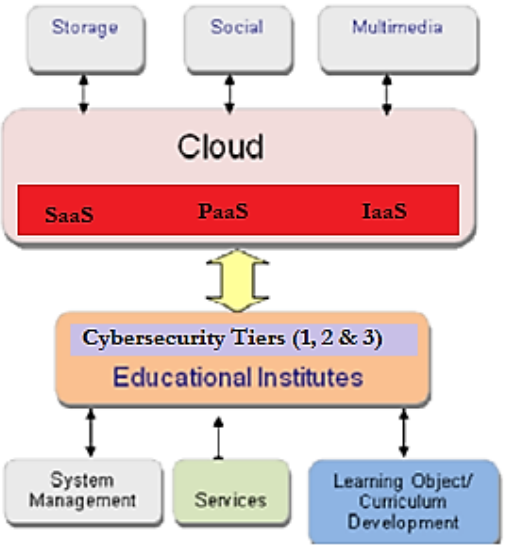

Figure 4. The cloud base online learning LMS (Source: [2]).

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

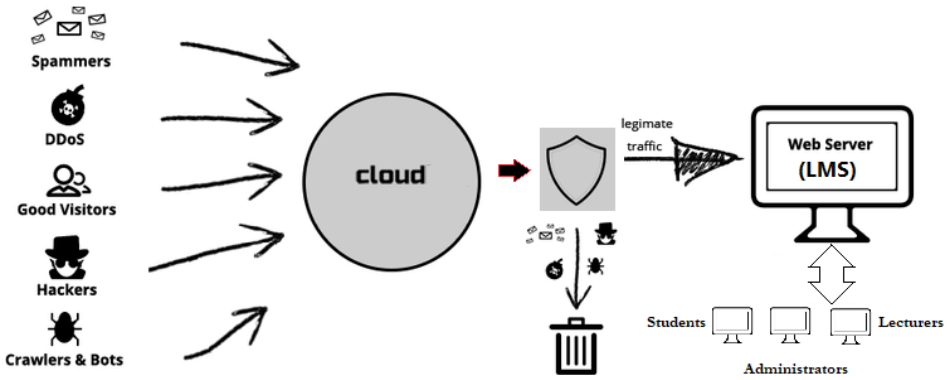

Figure 5. An example of the functionality of the proposed conceptual framework.

The findings in Section 3.1 led to the investigation of a conceptual framework for cloud based online learning architecture or the LMS architecture. Figure 3 represents a proposed cloud based LMS architecture which was adopted and adapted [2]. In this conceptual framework the cybersecurity layer was proposed to be included before the online learning users (education institutions clients) could access the cloud. This will make sure that the online learning users do not depend on the cloud computing's security policies, but they have a first layer of security that defends them before accessing the cloud. The latter creates a two (2) tier of protection meaning that cloud-based protection will happen together with on-premises protection as illustrated in Figure 4. The Tier 1 cybersecurity deals with initial incidence, incident responses and Tier 2 cybersecurity deals with threats, data damage or loss. With machine learning prediction has made it possible for the cybersecurity to be predicted either from the defenders' side or attackers' side. In this regard, Tier 3 support Tier 1 and Tier 2, as well as dealing with the use of cybersecurity tools to conduct predictions, anomaly detection, privacy paradox, and classification. In this regard, the proposed conceptual framework will align to the NIST security framework [28-29].

4. CONCLUSION

Since cloud based online learning is made up of technologies that could be vulnerable to cybersecurity. This paper used the literature review to source the importance of cybersecurity in cloud based online learning. It found that the issues of cybersecurity on cloud based online learning are still prevalent and could easily be thematically categorized.

The obtained themes were validated through a brief questionnaire-based activity with the professionals that involved in the online learning environment. The

findings corroborate the themes to be factful. Using both the SLR and the validation method, a 2-tier conceptual framework was proposed. The future studies will concentrate on contributing a 3-tier (prediction and detection of threats and attacks) within the cloud based online learning. The latter will help to identify and deal with cybersecurity cloud based online learning issues before they could happen.

REFERENCES

[1] S. Okai-Ugbaje, K. Ardzejewska, A. Imran, A. Yakubu and M. Yakubu. Cloud-based m-learning: A pedagogical tool to manage infrastructural limitations and enhance learning. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, vol. 16(2), p. 48-67, 2020.

[2] W.Q. Qwaider, "A Cloud Computing Based Learning Management Systems (LMSs) Architecture". *International Journal of Computing and Network Technology*, 5(2), p. 51-58, 2017.

[3] A. Ekuase-Anwansedo, and A. Smith, "Effect of Cloud Based Learning Management System on The Learning Management System Implementation Process". *SIGUCCS '19: Proceedings of the 2019 ACM SIGUCCS Annual Conference*, p. 176–179, 2019. https://doi.org/10.1145/3347709.3347835

[4] M. Rajesh, "A Systematic review of cloud security challenges in Higher Education". *The Online Journal of Distance Education and e-Learning*, p. 10, 2017.

[5] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering". *Information and Software Technology*, 2013.

[6] M. Kaur and H. Singh, "A Review of Cloud Computing Security Issues". *International Journal of Grid Distribution Computing*, vol. 8, p. 215-222, 2015.

[7] T.-S. Chou, "Security threats on cloud computing vulnerabilities". *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 5, 2013.

[8] J. Jang-Jaccard, S. Nepal, and Y. J. Guo, "Cybersecurity threats in cloud computing". *Australian Journal of Telecommunications and the Digital Economy*, vol. 1, 2013.

[9] M. Attaran, S. Mohsen and B. G. Celik, "Promises and Challenges of Cloud Computing in Higher Education: A Practical Guide for Implementation". *Journal of Higher Education Theory and Practice*, vol. 17(6), 2017.

[10] Y. A. M. Qasem, R. Abdullah, Y.Y. Jusoh, R. Atan, and S. Asadi, "Cloud Computing Adoption in Higher Education Institutions: A Systematic Review" *IEEE Access*, vol. 10, 2019.

[11] G. Kumar and A. Chelikani, "Analysis of security issues in cloud-based e-learning". Security Management, 2011.

[12] H. Takabi, J. B. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments". *The IEEE Computer and Reliability Societies*, 2010.
[13] C. N. Magdalena, "E-learning Security Vulnerabilities". *Procedia - Social and Behavioral Sciences*, vol. 46, p. 2297 – 2301.2012.
[14] R. Khalil, A. E. Mansour, W. A. Fadda, K. Almisnid, M. Aldamegh, A. Al-Nafeesah, A. Alkhalifah and O. Al-Wutayd, "The sudden transition to synchronized online learning during COVID-19 pandemic in Saudi Arabi: a qualitative study exploring medical students' perspectives". *BMC Medical Education*, 2020.
[15] H. Abusaimeh, "Security Attacks in Cloud Computing and Corresponding Defending Mechanisms". *International Journal of Advanced Trends in Computer Science and Engineering*, 2020.
[16] E. Bagarukayo and B. Kalema, "Evaluation of elearning usage in South African universities: A critical review". *International Journal of Education and Development using Information and Communication Technology*, 2015.
[17] I. Bandara, F. Ioras and K. Maher, "Cyber security concerns in E-learning education". *Proceedings of ICERI2014 Conference*, 17-19 November 2014.
[18] V. Chang, Y. Kuo and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds". *Future Generation Computer Systems*, 2016.
[19] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities". *The IEEE Computer and Reliability*, 2011
[20] P. Chouhan and R. Singh, "Security Attacks on Cloud Computing With Possible Solution". *International Journal of Advanced Research in Computer Science and Software Engineering*, 2016.
[21] A. Jalal and M. A. Zeb, "Security Enhancement for e-Learning Portal". *International Journal of Computer Sciences and Engineering Systems*, 2015.
[22] F. Makoza, "Cloud computing adoption in Higher Education Institutions of Malawi: An exploratory study". *International Journal Computing and ICT Research*, vol 9(2), 2016.
[23] R. P. Madhubala, "Survey on Security Concerns in Cloud Computing". *International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015.
[24] M. V. Pawar and J. Anuradha, "Network Security and Types of Attacks in Network". *Procedia Computer Science*, vol. 48, pp. 503 – 506, 2015. https://doi.org/10.1016/j.procs.2015.04.126
[25] K. Van der Schyff and K. E. Kraussy, "Higher education cloud computing in South Africa: Towards understanding trust and adoption issues". *South African Computer Journal (SACJ)*, 55 40-55, 2014.
[27] D. R. Queiros and M. R. de Villiers, "Online Learning in a South African Higher Education Institution: Determining the Right Connections for the Student". *International Review of Research in Open and Distributed Learning*, 2016.

[28] P. Mell and T. Grance, "The NIST Definition of Cloud Computing". National Institute of Standards and Technology Recommendations of the National Institute of Standards and Technology, 2011.
[29] National Institute of Standards and Technology Cybersecurity Framework Documents. https://www.nist.gov/cyberframework/framework