**Security risks in Cloud-based e-learning: A Literature Review**

**Abstract**

Cloud computing derives from distributed computing. It aims to provide access to computing resources by offering a variety of cloud structures (models) and services. The models and services available have changed the way education material an sessions are delivered to students, making the availability and interaction two of its key benefits. However, these benefits come together with security risks that are related to giving the control of internal data to a third party company.

This review examines the risks of using e-learning information systems based on the cloud. Most authors focussed on security and categorise the risks according to the cloud model used. A large number of articles focus on the infrastructure and only a small percentage on the security.

Although the cloud offers services to systems used in different sectors, educational systems will face their own types of security risks, such as manipulation, authentication and confidentiality. Added to this, The type of model on which the solution is based will determine the type of threats this will be exposed to.

Despite the vast number of advantages the cloud offers when implementing e-learning systems, the security concerns remain the most important for organisations.

**Introduction**

With early foundations in the 1960s, research in virtualisation, operative systems, storage, and networking in the 1970s and 1980s, the maturity of its foundational technology in the 1990s, the introduction of the modern concepts of cloud computing were materialised by the launching of Amazon Web Services (AWS) in the early 2000s (Varghese, 2019). The modern cloud computing models SaaS, IaaS, and PaaS provide service solutions for different enterprise requirements. As flexibility is one of the main characteristics of cloud computing, the solutions will vary from one organisation to another. The levels of scalability, control, and security are different for different implementations.

Storing data on the cloud, where multiple locations potentially exist, represents a security risk. Security risks are associated with some of the fundamental elements of cloud computing, such as virtualisation, limited visibility, and multiple locations. These risks can also include data loss and data breaches.

In modern educational systems, mobile, distance and web-based learning are essential and driven by cloud services (Paul et al., 2023). Collaboration is another crucial concept in e-learning; it allows students to interact and work together on tasks assigned by the teachers. Here, the concept of flexibility becomes essential because it makes the mentioned interaction possible. All these benefits can put the security of data at risk, and although cloud service providers invest a lot in security measures, risks are still a problem to solve.

**In this review, we focus on the security risks that affect the e-learning activities of educational organisations that have moved their services to the cloud, the challenges they face and the actions they take to mitigate or prevent the effects of potential threats.**

**Methodology**

A chronological approach has been used to analyse and synthesise a number of research articles related to the security risks of using cloud-based e-learning systems.

**Objective**

**The objective of this literature review is to present relevant insight through an overview of the most concerning security risks that affect cloud-based e-learning. For this, we have covered the concepts of cloud, e-learning, cloud-based e-learning, and security risks.**

**Literature review**

Cloud computing is a model that allows the quick provision of resources (network, servers, storage, etc.) in a ubiquitous, convenient, and on-demand way, with minimal intervention from the service provider (Ruparelia, 2016). The use of the cloud in education has many positive effects, and this applies to all types of entities implementing solutions based on this technology.

According to (Oracle, N.D.), the benefits of Could Computing are:

* Accessibility
* Makes it possible to use it with minimum in-house software and hardware
* Centralised data security
* High performance and availability
* Quick application deployment
* Instant business insights
* Business continuity
* Price-performance and cost savings

E-learning based on cloud services has the potential to reduce not just the development team cost but also the technical support team cost, testing effort, requirement elicitation, scheduling backup management, and cost of the overall project (Ahmed, 2015). Benefits of Cloud in the education sector (e-learning)

* Easy access
* Access from various type of devices
* Students can collaborate
* Teachers can offer targeted content
* Virtualisation
* Centralised storage
* Lower cost
* Enhanced performance
* Fast updates
* Better compatibility
* Continuous backup

The importance of cloud computing in enhancing e-learning cannot be doubted. With Cloud technology as the base of e-learning, the whole system can offer access to massive data collections, flexibility and allow users to do modifications, test, and associate with various types of software use of different methods that otherwise would require educational organisations to buy separate software licenses and hardware to support them (Burney & Alam, 2020).

**Review**

Multiple researches on cloud-based e-learning systems have suggested lists of the main security risks these types of systems face. The risks are associated with the core cloud technology, but the different levels of importance are determined (or aggravated) by the specific activities of e-learning.

E-learning collaborative systems are typically designed and implemented without security as their primary concern but with pedagogical principles as the most important (Bandara, 2014). These definitions refer to all types of e-learning systems, whether cloud-based or not. Security measures are nowadays embedded in cloud services; for example, security policies will need to be defined to allow specific devices to connect to the service. However, as security is ongoing, static measures can never guarantee the maximum level of security.

The article (Manimaran, 2015) presents a list of security issues categorised by cloud model type. This study also provides a model that implements a secure layer to secure an e-learning environment. This layer, located between the e-learning users and the cloud provider, acts as a defence against insider attacks, flooding attacks, VM attacks and BDC attacks. Also, this research focuses on data availability and points to the DoS attacks as the root of all availability attacks. (Divya, 2015) Highlights the requirements to achieve confidentiality, integrity and availability. Confidentiality can be achieved by using encryption and protecting authentication details. Choosing a cloud provider that ensures robust atomicity, consistency, isolation and durability (ACID) characteristics can help achieve integrity. Availability by preventing attacks such as DoS and providing resilience to the network. The authors analyse the available cloud-based e-learning models and conclude that the proposed architectures and the lack of guidance regarding security concerns are common issues.

The article (Malik et al., 2016) approaches the cloud-based e-learning security issues from the users point of view by exposing their crucial security concerns. This study introduces an Improved Access Mechanism for authentication (biometrics) and a ACL to assign access to the relevant users. The ‘Education plus Training concept’  discussed in this study, results very important as it takes into account the human factor and add it to their proposed model.

(Kanimozhi et al., 2018) Propose an implementation focusing on access control to overcome the fact that users or participants can access the system and share content from different countries, meaning that the source environment can vary. The authors also include the concept of Key Management Schemes to ensure the protection of the shared data. The authors of (Hussen et al., 2019) discuss recent security issues in relation to implementing cloud-based e-learning systems and propose a novel model to improve not just the security but also the whole quality of e-learning in universities. They also describe the security issues based on the Cloud model.

In (Onyema et al., 2020), The authors indicate that the security risks mainly come from the cloud infrastructure and also the means used to access the services and systems. As the connection to the services is made over the internet, networks can present vulnerabilities that could result in different types of attacks such as DoS, Data leakage, spoofing, malware injection, etc. In the study (Bruma, 2020), the author analyses the principal vulnerabilities that affect cloud computing against the security methods used currently on cloud-based e-learning systems, concluding that security attacks mainly happen when security breaches caused by technology vulnerabilities and misconfigured network equipment are exploited.

(Najm et al., 2022) provides a detailed list of potential risks on cloud-based e-learning systems, divided by two criteria: having the infrastructure as a target (causing harm to a number of users) and having the individual as a target (causing harm to the targeted person). This is very useful as the authors classify the risks according to the cloud model, which clarifies the understanding of the risks. (Malele, 2023) presents a literature review on cybersecurity cloud-based online learning; the study found that confidentiality, integrity, and availability issues are a concern and that this led to issues of security awareness, authentication, and blended attacks. (Chatterjee et al., 2023) The use of cloud-based educational systems that use the Learning Management System (LMS) is revealing an increase due to the concurrency associated with its use. This study focuses on using an LMS to provide enhanced levels of security to all users involved, based on the Cloud attack, the cryptographic, and steganographic models.

According to (Eljak et al., 2024), most of the studies about the impact of moving the e-learning system to the cloud focus on the infrastructure (27%) and only 4% focus on security. The article by (Nicola et al., 2024) also presents data integrity, access control, location of data, Loss of data, and service traffic as the most relevant risk concerns. The authors also present ideas of solutions or mitigations for the mentioned security concerns. Finally, the authors also remark on the need to have enhanced mechanisms of security for educational organisations so the levels of security can be increased without affecting performance.

The dynamic nature of cloud technology changes also dynamically affects the appearance of security risks. After reviewing the present literature, we haven’t found sufficient information on specific security risks in e-learning. Most authors agree on the main sources of security risks in cloud-based e-learning systems, but only a few recommend the creation of a framework to deal with and prevent attacks.

**Conclusions**

This literature review covers papers and articles from 2015. We can appreciate that cloud providers have now covered security risks and concerns discovered over the years. For instance, leading cloud providers have implemented security measures to protect data availability. This is not to say that no measures should be taken, but to remark on the dynamic nature of the security field.

While an analysis of the infrastructure and connectivity means of current cloud providers is necessary, the absence of a well-defined systemic approach to minimize risks in cloud-based systems presents a clear opportunity for future research.

Some other concerns that can bring about the advent of Communication as a service (CaaS), Desktop as a service (DaaS), and Function as a service (FaaS) will need to be addressed to keep the system's security at an acceptable level. This will depend on the cloud model on which the e-learning system would be based.

**References**

Ahmed, F. (2015) Comparative Analysis for Cloud Based e-learning . *International Conference on Communication, Management and Information Technology*  65: 368-376. DOI: https://doi.org/10.1016/j.procs.2015.09.098

Bandara, I. (2014). CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION. *International Conference of Education, Research and Innovation.* DOI: http://dx.doi.org/10.13140/2.1.4451.3604

Bruma, L. (2020)  SECURITY VULNERABILITIES IN CLOUD BASED E-LEARNING. *eLSE 2020*. 190-197.  DOI: http://dx.doi.org/10.12753/2066-026X-20-024

Burney, s.M.Aqil & Alam, F. (2020). THE IMPACT OF CLOUD COMPUTING ON e-LEARNING. DOI: http://dx.doi.org/10.13140/RG.2.2.24749.92649

Chatterjee, P., Bose R., Banerjee, S. &  Roy, S. (2023) Enhancing Data Security of Cloud Based LMS. Wireless Personal Communications 130:1123–1139. DOI: https://doi.org/10.1007/s11277-023-10323-5

Divya, P. & Prakasam, S. (2015) Effectiveness of Cloud based E-Learning System (ECBELS). *International Journal of Computer Applications.* 119(6). Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=42ba64739b2f49910434ee96b59fb17f78c77c12 [Accessed 17 April 2024]

Eljak, H., Ibrahim A. O., Saeed, F., Hashem I. A. T., Abdelmaboud, A., Syed H. J., Abulfaraj, A. W., Ismail M. A. B., Elsafi, A. (2024) E-Learning-Based Cloud Computing Environment: A Systematic Review, Challenges, and Opportunities. *IEEE Access*, vol. 12, pp. 7329-7355. DOI: https://doi.org/10.1109/ACCESS.2023.3339250.

Hussen, M. O., Sharma, N., El-Sofany H. F. (2019) A NOVEL MODEL FOR SECURING ACCESS OF CLOUD-BASED E-LEARNING SYSTEMS. International Journal of Engineering Applied Sciences and Technology, 2019. 4(7) 1-9. Available from: https://ijeast.com/papers/1-9,Tesma407,IJEAST.pdf

Kanimozhi, S., Arputharaj, K.,  Devi, K. & Selvamani, K (2018). Secure cloud-based e-learning system with access control and group key mechanism. *Concurrency and Computation: Practice and Experience.* 31(3). DOI: http://dx.doi.org/10.1002/cpe.4841

Malele, V. (2023). Cybersecurity Cloud-Based Online Learning: A Literature Review Approach. *Journal of Information Systems and Informatics*, 5(4), 1623-1632. DOI: https://doi.org/10.51519/journalisi.v5i4.583

Malik, A., Sarfraz, S., Shoaib, U., Abbas, G., & Sattar, M. (2016). Cloud based E-Learning, Security Threats and Security Measures. *Indian Journal of Science and Technology.* 9(48). DOI: http://dx.doi.org/10.17485/ijst/2016/v9i48/96166

Manimaran, A. (2015) A Study on Security Issues in Cloud Based E-Learning. Indian Journal of Science and Technology. 8. 757–765. DOI: http://dx.doi.org/10.17485/ijst/2015/v8i8/69307

Najm,Y., Alsamaraee, S., & Jalal, A. (2022). Cloud computing security for e-learning during COVID-19 pandemic. *Indonesian Journal of Electrical Engineering and Computer Science*. 27. 1610-1618. DOI: http://dx.doi.org/10.11591/ijeecs.v27.i3.pp1610-1618

Nicola, A., Elmagadi, A., Bushara, N., Saeed, E. (2024) Obstacles Challenge Investigating Scope in Cloud Based Distance Education System of the Quality of Services. Available from: https://www.eimj.org/uplode/images/photo/moneer5000@yahoo.com..pdf [Accessed 19 April 2024]

Onyema, E.  Nwafor, Ugwugbo,  Afriyie, R. & Ogbonnaya, Uchenna. (2020). Cloud Security Challenges: Implications on Education. 9. 56-73.

Paul, P.K., Aithal P.S., Chatteriee, R. & Saavedra, R. (2023). Cloud Computing and its Impact in Education, Teaching and Research-A Scientific Review. DOI: http://dx.doi.org/10.5281/zenodo.8078784

Quadri, N. & Ahmad, N. (2019). Critical Success Factors (CSFs) for Cloud-based E-Learning. *International Journal of Emerging Technologies in Learning (iJET)*. 14(01): 140. DOI: http://dx.doi.org/10.3991/ijet.v14i01.9170

Ruparelia, N. (2016) Cloud Computing. Available from: https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf [Accessed 16 April 2024]

Salimovna, F. D. , Salimovna Y. N., &  Ugli I. S. Z. (2019) Security issues in E-Learning system. *2019 International Conference on Information Science and Communications Technologies (ICISCT)* pp. 1-4, DOI: https://doi.org/10.1109/ICISCT47635.2019.9011971

Varghese, B. (2019) History of the Cloud. Available from: https://www.bcs.org/articles-opinion-and-research/history-of-the-cloud/ [Accessed 14 April 2024]