**Key security risks when adopting AIaaS cloud service model in cloud-based e-learning systems**

**Introduction & Research problem**

It is well known that a vast percentage of security risks are transferred from the underlying technology used for implementing systems. Cloud computing is not the exception, and it presents several security concerns, such as Data Location, User Access Privileges, and Data Segregation (Balani & Varol, 2020). At this point, we must consider the perspective of the education environment, where some risks can represent concerns that are more important than those in other industries. In this regard, we have found that in the case of e-learning systems, security risks are linked mainly to the confidentiality and integrity of data.

AIaaS is defined by Lins et al. (2021) as a cloud-based system that provides AI as a service to allow organisations and individuals to implement, deploy, train, and manage AI models. This service represents a cost-effective way to implement AI without risking investing large amounts of money in creating the underlying infrastructure from scratch.

According to (Lins et al., 2021), AIaaS carries usual risks inherent to cloud computing, specially lack of control and security concerns. But also, the deployment of AI based systems can potentially present threats (Alawadhi et al., 2022). This situation makes important to find the specific security risks associated to each technology in order to find a balance between risks and benefits.

From our preliminary literature review, we concluded that most leading cloud providers have implemented security measures to protect data availability. The advent of new cloud service models such as AIaaS and its potential inclusion in implementation of cloud-based e-learning systems can bring new security concerns to this type of systems.

The present literature also revealed insufficient information on specific security risks in e-learning. Most authors agree on the primary sources of security risks in cloud-based e-learning systems, but only a few recommend creating a framework to deal with those security risks and prevent attacks.

**Importance & Significance**

Finding an understanding the security risks inherent to the used of AIaaS as part of a cloud-based e-learning is important to the organisation decision makers. The decision to adopt this relatively new cloud service model needs to be supported by a previous knowledge of the key security risks and their impact in the new or future e-learning system.

This research will contribute with new knowledge on the security risk when cloud computing models and AI are used together, in our case, implemented and offered as AIaaS. Different categories of AIaaS can bring different types of risk, and it is necessary to understand these differences in order to propose mitigations to their effects. The findings of this research could potentially contribute to the development of a security framework that takes into account specific aspects of cloud-based e-learning systems.

**Research question**

Following the previous discussion, we can infer that by using AI over cloud computing can produce a combined set of security risks. These security risks need to be assessed and reduced so more organisations can confidently migrate to cloud-based e-learning systems that use the advantages of AI. This constitutes the reason for doing the proposed study.

**Research aim**

This research seeks to identify key security risks when including Artificial Intelligence as a Service (AIaaS) in the implementation of cloud-based e-learning systems. Through this process, we aim to produce awareness and guidance for the professionals involved in the implementation of this type of systems.

**Research objectives**

* To provide a comprehensive review of security risks that affect cloud implementation in general
* To provide a review of security risks that affect the implementation of cloud-based e-learning systems.
* Analyse new literature that includes potential risks in the introduction of the relatively new cloud service model AIaaS when implementing cloud-based e-learning systems.
* Study the impact of potential future security events using Scenario analysis to produce different outcomes that will allow us to respond to different security threats.

**Methodology**

The proposed research methodology will be based in the analysis of primary and secondary resources. Primary resources like security reports from organisations that have implemented AIaaS not just at the level of bots and assistants but also at the level of machine learning (ML) and application programming interfaces (APIs). Secondary resources like scientific articles that analyse the security risks inherent to solutions that combine AIaaS and cloud-based e-learning systems.

To evaluate possible events related to security risks, we will use Scenario analysis as a base technique. Scenario analysis identifies, measures and provides means to respond to the potential occurrence of different future risk events (Airmic, 2023). We have chosen this technique because it not only analyses the impact of potential events but also because  it provides a ‘what if’ thinking analysis. This forward thinking aligns with the nature of security risks.

The proposed research philosophy is Epistemology. This will be qualitative research, and we aim to produce new knowledge. This philosophy will guide us on choosing the most appropriate research sources and  on how to gather knowledge from them.

**Ethical considerations**

A few ethical concerns when accessing primary resources are covered by ensuring confidentiality and integrity and informing the relevant actors about the results of this research.

The reports provided by Organisations will be kept under strict confidentiality control and only authorised content will be published. All the secondary resources will be referred in the final research document, and finally, the results of the research will be communicated to the participants.

**Gantt diagram**

****

**References**

Airmic (2023). Scenario Analysis, A Practical Guide. Available from: https://www.airmic.com/system/files/technical-documents/Airmic-Scenario-Analysis-Guide.pdf [Accessed 15 May 2024]

Balani, Z. & Varol, H. (2020). Cloud Computing Security Challenges and Threats. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-4. DOI: http://dx.doi.org/10.1109/ISDFS49300.2020.9116266

Lins, S., Pandl, K., Teigeler, H., Thiebes, S., Bayer, C., & Sunyaev, A. (2021). Artificial Intelligence as a Service. *Business & Information Systems Engineering*. 63(4):441–456. DOI: <https://link.springer.com/article/10.1007/s12599-021-00708-w>

**Intro**

Following my literature review assignment where I chose Security risks in Cloud-based e-learning: A Literature Review, for this assignment I chose the title Key security risks when adopting AIaaS cloud service model in cloud-based e-learning systems

I have divided this presentation in different parts according to the nature of this intended research.