

**Proactive intrusion detection approach
in hybrid cloud environments using
artificial intelligence**

Prepared by

ALI MMADI, PhD student - Midocean University



Research Skills (2)

Task 2

ALI MMADI

PhD student - Midocean University

www.midocean.ae

1.Introduction and announcement of the topic

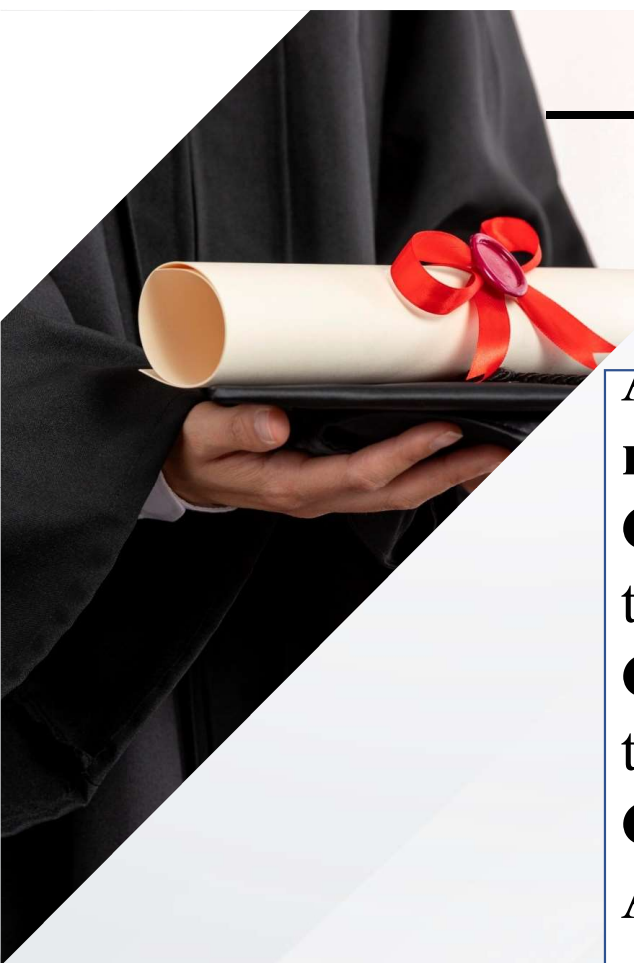
Hello everyone, My name is **Ali Mmadi**, a PhD student in **Information Technology**, specializing in **Cybersecurity**.

In this second task,

I will present a scientific research entitled: "**Proactive Intrusion Detection Approach in Hybrid Cloud Environments Using Artificial Intelligence**."

I will analyze three essential elements of this research:

- **First, the scientific title and its relevance,**
- **Then, the introduction and its writing quality,**
- **Finally, the research problem and the method used to formulate it.**



2. Scientific standards for writing a research title

According to international scientific standards, a good **research title should be:**

Clear and precise: it should reflect the actual content of the research.

Comprehensive: it should mention the main variable, the context, and the method or technology used.

Concise: avoid titles that are too long or vague.

And scientifically formulated, meaning that it expresses a research idea rather than a simple description. In our case, the title 'Proactive Intrusion Detection Approach in Hybrid Cloud Environments Using Artificial Intelligence' is scientifically correct.

Why?

- ☐ It presents the main theme: **intrusion detection.**
- ☐ It specifies the context: **hybrid cloud environments.**
- ☐ And it indicates the method or technology used: **artificial intelligence.**

This title is therefore **complete, specific, and measurable**, as it suggests a clear objective — proactive detection — and announces the field of application (the Cloud) as well as the technological approach (AI).

3. Analysis of the Introduction

Let's now move on to the introduction.

In scientific writing, a good introduction should follow a logical three-step structure:

- 1) The general context of the field, to situate the research.**
- 2) The justification of the problem, that is, why this topic is important.**
- 3) The transition to the objectives or the research question.**

possible introductory summary

"With the widespread adoption of hybrid Cloud infrastructures, companies simultaneously host their data across multiple public and private environments.

This interconnection expands the attack surface and makes systems more vulnerable to sophisticated intrusions.

Despite advancements in traditional cybersecurity tools, detection mechanisms often remain reactive. In this context, the use of artificial intelligence and machine learning enables the design of proactive detection systems capable of identifying abnormal behaviors before an attack occurs."

In my opinion, this **introduction is solid** because:

- ☐ **It clearly sets the overall context,**
- ☐ **It justifies the relevance of it guides towards the topic,**
- ☐ **And the proposed solution (AI for cybersecurity).**

It therefore adheres to the **correct principles of scientific writing**: clarity, coherence, justification, and logical progression.

4. Presentation and evaluation of the research problem

The research problem is at the heart of any scientific work. For this topic, the problem can be formulated as follows:
"How can we design a system capable of proactively detecting complex intrusions in a hybrid Cloud environment, using artificial intelligence models that can learn normal behaviors and anticipate attacks?"

This formulation meets three methodological criteria:

Specificity: the problem focuses on proactive detection and hybrid Cloud. Scientific relevance: it is part of a current global cybersecurity issue. Feasibility: it is achievable with modern tools such as neural networks, machine learning, or intelligent IDS/IPS systems. The method for selecting the problem follows the classic scientific approach:

Observation of the limitations of existing security systems, Identification of the need for anticipation in intrusion detection, Then formulation of a clear problem related to cybersecurity performance and prediction. The problem is therefore well-defined, measurable, and aligned with the field of applied cybersecurity.

5. Conclusion and outlook

In summary:

- The title meets scientific standards as it is clear, comprehensive, and precise.
- The introduction is strong, as it presents the context, justifies the research, and guides toward the objectives.
- The research problem is well-defined and scientifically relevant, with a logical and coherent method.
- This type of study directly contributes to strengthening cloud infrastructure cybersecurity, a crucial area for the protection of data and critical services in the digital age.

Bibliographic reference

- 1) Scarfone, K., & Mell, P. (2021). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94. <https://csrc.nist.gov/publications/detail/sp/800-94/final>
- 2) Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach for Intrusion Detection in Cloud Environments. Future Generation Computer Systems, 89, 347–359.
- 3) He, H., & Chan, S. (2022). Hybrid AI Models for Cloud Intrusion Detection: A Review. IEEE Access, 10, 20315–20329.
- 4) Shastri, A., & Gaur, M. S. (2023). AI-based Threat Prediction in Hybrid Clouds. Journal of Information Security Research, 14(1), 25–41.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

