



Task 7 Proposed topic

*“Integration of Machine Learning, Zero Trust Architecture,
and Cyber Resilience for Intrusion Detection in Hybrid Cloud
Environments”*

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues(3)

Task 7

ALI MMADI

PhD student - Midocean University

www.midocean.edu.km

Introduction

In this assignment, I will present and analyze the main theoretical frameworks related to my research topic, which focuses on the use of artificial intelligence for the detection of cyberattacks in hybrid cloud environments. The objective is to assess the relevance of these theoretical frameworks and to propose an integrated conceptual model.



1. Presentation of the theoretical frameworks

1. Machine Learning in cybersecurity

Machine Learning is today widely used to detect anomalies and attacks.

It allows:

- automatic analysis of large amounts of data
- detection of suspicious behaviors
- continuous improvement of security systems

However, it has some limitations:

- dependence on training data
- risk of overfitting
- difficulty in explaining decisions

Zero Trust Architecture

The Zero Trust model is based on the principle:
“Never trust, always verify”

It requires:

- ❖ continuous authentication
- ❖ strict access control
- ❖ constant monitoring

This model is particularly suitable for hybrid cloud environments.

But its limitations include:

- ☐ implementation complexity
- ☐ high costs
- ☐ dependence on proper configuration

Cyber Resilience

Cyber resilience aims to:

- ❖ anticipate attacks
- ❖ withstand incidents
- ❖ recover quickly

It complements traditional security approaches.

However, it remains difficult to measure quantitatively.

2. Critical analysis of theoretical frameworks

These three frameworks are complementary but have individual limitations:

Machine Learning is effective but depends on data

Zero Trust improves security but increases complexity

Cyber resilience is strategic but difficult to implement

➤ No single approach is sufficient

Therefore, integration is necessary.

3. Proposal of the conceptual model

I propose a conceptual model based on three layers:

- ❑ **Layer 1:** Intelligent Detection (Machine Learning)Anomaly identificationReal-time analysis
 - ❑ **Layer 2:** Access Control (Zero Trust)Continuous verificationAccess limitation
 - ❑ **Layer 3:** ResilienceIncident responseRapid recovery
- This model allows for complete security:
Prevention + Detection + Response

4. Research hypotheses

✓ **Main Hypothesis (H1)**

The integration of Machine Learning with the Zero Trust architecture significantly improves the accuracy of cyberattack detection in hybrid cloud environments.

✓ **Main Hypothesis (H2)**

The addition of cyber resilience mechanisms reduces the impact of cyberattacks and improves recovery time.

✓ **Secondary Hypothesis (H3)**

Lightweight Machine Learning models offer better performance in resource-constrained environments.

5. Relevance of the model for research

This model is relevant because:

- ☐ it addresses the limitations of existing Approaches
- ☐ it incorporates current research trends
- ☐ it is adaptable to real-world environments

It also allows for:

- ❖ greater overall
- ❖ Safety a reduction of risks
- ❖ an improvement in performance

6. Limits of the theoretical framework

Despite its advantages, this model has certain limitations:

- ❑ **Integration Complexity**

Combining several approaches can be technically difficult

- ❑ **Scalability**

The model can be difficult to deploy on a large scale

- ❑ **Human Factor**

Human errors remain a major risk

Conclusion

In conclusion,

The theoretical frameworks analyzed show that modern cybersecurity requires an integrated approach.

The proposed model combining Machine Learning, Zero Trust, and cyber resilience constitutes a solid basis for addressing current challenges.

It offers a theoretical and practical contribution to cybersecurity research.

Thank you for your attention.

Key References (APA)

Sarker, I. H. (2023).

AI-based cybersecurity: A comprehensive review.

Rose, S., et al. (2020).

Zero Trust Architecture (NIST SP 800-207).

Linkov, I., & Kott, A. (2019).

Cyber resilience fundamentals. *IEEE Security & Privacy*.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

