



Task 8 Proposed topic
“Design of an Intelligent and Lightweight Cyberattack Detection System for Hybrid Cloud Environments Based on Machine Learning and Zero Trust Architecture”

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues(3)

Task 8

ALI MMADI

PhD student - Midocean University

www.midocean.edu.km

In this assignment, I present a complete research proposal in the field of cybersecurity, focusing on the intelligent detection of cyberattacks in hybrid cloud environments.

This research aims to propose an innovative solution combining artificial intelligence, Zero Trust architecture, and cyber resilience.

1. Research problem

With the growth of hybrid cloud, IT systems are becoming more complex and vulnerable.

Traditional security systems are no longer sufficient in the face of:

- ☐ the evolution of cyberattacks
- ☐ the massive volume of data
- ☐ internal threats

➤ Main problem :

How to design an intelligent system capable of effectively detecting cyberattacks in a hybrid environment while being suitable for limited resources?

2. Research objectives

❖ Main Objective:

Develop an intelligent AI-based intrusion detection model that is efficient and lightweight.

❖ Specific Objectives:

- ☐ Improve detection accuracy
- ☐ Reduce false positives
- ☐ Optimize real-time performance
- ☐ Integrate Zero Trust into detection

3. Research hypotheses

✓ **H1:**

The integration of Machine Learning significantly improves the detection of cyberattacks.

✓ **H2:**

The Zero Trust architecture reduces unauthorized access.

✓ **H3:**

A lightweight model is better suited for resource-limited environments.

4.Theoretical framework

This research is based on three pillars:

- Machine Learning
- Zero Trust
- Cyber Resilience

These concepts are integrated into a combined conceptual model.

5. Research methodology

Type of research:

Quantitative and experimental

Steps: Data collection:

- UNSW-NB15
- CICIDS2017

Preprocessing:

- Cleaning
- variable selection

Modeling:

- Random Forest
- SVM
- Light Deep Learning

Evaluation: Criteria used: Accuracy, Precision, Recall, F1-score, Response time

6.Expected results

- ☐ Precision $> 90 \%$
- ☐ Reduction of false positives $> 25 \%$
- ☐ Improvement in detection time

The model will be more efficient than traditional systems

7. Scientific contribution

This research provides:

- ☐ An innovative combined model
- ☐ A solution adapted to developing countries
- ☐ An improvement of existing systems

8. Limitations of the research

- ❖ Limited external validity
- ❖ Difficulty of large-scale deployment
- ❖ Influence of the human factor

9. Practical importance

- ❖ This project can be used in:
- ❖ public administrations
- ❖ Companies
- ❖ critical infrastructures

It helps improve the overall security of systems.

10. Implementation plan

- ❖ **Phase 1:** Literature review
- ❖ **Phase 2:** Data collection
- ❖ **Phase 3:** Model development
- ❖ **Phase 4:** Evaluation
- ❖ **Phase 5:** Writing

Conclusion

In conclusion,

This research proposes a comprehensive and innovative solution to improve cybersecurity in hybrid environments.

It combines theory and practice, and addresses the current challenges of modern cybersecurity.

you for your attention.

Key References (APA)

Sarker, I. H. (2023).

AI-based cybersecurity: A comprehensive review. *Journal of Network and Computer Applications*.

Sharma, A., & Chen, J. (2024).

Machine learning for cyber threat detection. *Computers & Security*.

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

Zero Trust Architecture. NIST.

Sharafaldin, I., et al. (2018).

CICIDS2017 dataset. *ICISSP*.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

