



Task 6 Proposed topic

“A Lightweight AI-Based Intrusion Detection Model for Hybrid Cloud Environments in Resource-Constrained Systems”

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues(3)

Task 6

ALI MMADI

PhD student - Midocean University

www.midocean.edu.km

Introduction

In this assignment, I present a research proposal in the field of cybersecurity, focusing on the use of artificial intelligence for detecting cyberattacks in hybrid cloud environments.

1. Research problem

With digital transformation, organizations are increasingly adopting hybrid architectures combining public and private clouds. However, these environments introduce significant vulnerabilities. According to recent studies, more **than 60% of cyberattacks target cloud environments**, and traditional detection systems are becoming ineffective in the face of the complexity and volume of data.

The main problem is therefore:

- How can we design an AI-based intrusion detection system that is efficient, scalable, and suitable for resource-constrained environments?

2. Importance of research

This research is important for several reasons:

- ❑ Rapid increase in cyberattacks
- ❑ Need for intelligent and automated solutions
- ❑ Lack of solutions adapted to developing countries

Furthermore, current solutions often require:

- ❖ significant computing power
- ❖ costly infrastructure

Which limits their adoption in certain contexts.

3. Research objectives

Main objective:

Develop an intelligent intrusion detection model adapted to hybrid cloud environments.

Specific objectives:

- Design a lightweight machine learning-based model
- Reduce the false positive rate Improve real-time performance
- Adapt the solution to resource-constrained environments.

4. Research questions

How can we improve detection accuracy while reducing computational costs?

Which AI algorithms are best suited for hybrid environments?

How can we integrate human factors into security systems?

5. Theoretical framework

This research is based on several concepts:

- ❖ **Machine Learning in cybersecurity**
- ❖ **Zero Trust Architecture**
- ❖ **Cyber Resilience**

These frameworks help to understand the mechanisms for detecting and responding to cyber threats.

6. Research methodology

The methodology adopted will be experimental and quantitative.

◆ Steps:

1. Data Collection:

- ☐ UNSW-NB15 Dataset
- ☐ CICIDS2017 Dataset

2. Data Preprocessing:

- ☐ Cleaning
- ☐ Feature Selection

3. Model Development:

- ☐ Algorithms Used:
 - Random Forest
 - Support Vector Machine
 - Lightweight Deep Learning

4. Evaluation:

Accuracy , Recall , F1-score , Detection Time

7. Expected results

The expected results are:

- ❖ **Improved accuracy (>90%)**
- ❖ **Reduced false positives (>25%)**
- ❖ **Decreased detection time**

The proposed model should be more effective in hybrid environments than traditional models.

8. Limitations of the research

This study has some limitations:

- ❑ External validity:

The datasets may not represent all real-world attacks.

- ❑ Scalability:

The model may be difficult to deploy on a large scale.

- ❑ Human factor:

Human error remains a major cause of vulnerability.

9. Scientific contribution

This research will provide:

- ❖ A model adapted to resource-constrained environments
- ❖ Improvements to existing detection systems
- ❖ A contribution to AI research in cybersecurity

Conclusion

In conclusion,

This proposal aims to address current cybersecurity challenges in hybrid environments.

It combines artificial intelligence, efficiency, and adaptation to real-world constraints.

It also paves the way for future research in the field of intelligent cybersecurity.

Thank you for your attention.

عيد مبارك

KEY REFERENCES

- 1) Sarker, I. H. (2023).
AI-based cybersecurity: A comprehensive literature review. *Journal of Network and Computer Applications*.
- 2) Sharma, A., & Chen, J. (2024).
Machine learning for cyber threat detection in hybrid cloud environments. *Computers & Security*.
- 3) Zhang, Y., et al. (2022).
Artificial intelligence in cloud security. *IEEE Access*.
- Sharafaldin, I., et al. (2018).
CICIDS2017 dataset. *ICISSP*.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

