



Task 9: Proposed topic

*“Analysis of a previous study in the light of theoretical frameworks
Selected Study”*

*Zhang, Y., Chen, X., Li, L., & Wong, D. S. (2022) Artificial Intelligence
in Cloud Security: A Survey – IEEE Access*

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues(3)

Task 9

ALI MMADI

PhD student - Midocean University

www.midocean.edu.km

In this assignment, I am going to analyze a previous scientific study in the field of cybersecurity, using specific theoretical frameworks. The chosen study focuses on the use of artificial intelligence in cloud security. The objective is to evaluate this study in light of three theoretical frameworks:

- ☐ Machine Learning
- ☐ Zero Trust
- ☐ Cyber Resilience

1. Presentation of the study

The study analyzes the use of artificial intelligence to improve security in cloud environments.

❖ **Objective:**

Identify the most effective AI techniques for cyber threat detection.

❖ **Methodology:**

- Systematic review of over 100 scientific articles
- Comparative analysis of algorithms
- Classification of security approaches

➤ **Results:**

- Deep Learning models achieve accuracy above 95%
- False positives reduced by up to 30%
- Improvement in detection time

2. Analysis according to the Machine Learning framework

- ❖ The study confirms that Machine Learning is a powerful tool for intrusion detection.

✓ **Strengths:**

- Ability to analyze large amounts of data
- Automatic anomaly detection
- High accuracy ($> 95\%$)

! **Limitations:**

- dependence on datasets
 - risk of overfitting
 - low explainability
- The study shows high effectiveness but a critical dependence on data.

3. Analysis according to the Zero Trust framework

The study indirectly addresses the Zero Trust model.

✓ **Positive points:**

- importance of continuous monitor
- ingneed to verify access

! **Limitations:**

- absence of explicit integration of the Zero Trust model
 - lack of analysis on access control
- The study is limited because it focuses on detection, not prevention.

4. Analysis according to the Cyber Resilience framework

The study hardly addresses cyber resilience.

Contributions:

- ☐ improvement of detection
- ☐ reduction of impacts

! Limits:

- ☐ lack of recovery strategies
- ☐ no continuity plan

The resilience dimension is insufficiently developed.

5. Analysis of the methodology

The study uses a systematic review, which is a rigorous method.

Advantages:

- wide analysis of the literature
- overall view of the field

! Limitations:

- ❖ lack of direct experimentation
- ❖ dependence on existing studies
- ❖ possible bias in article selection
- The results are solid but remain theoretical.

6. Interpretation of the results

The results show that:

- AI significantly improves detection
- advanced models offer better performance

However:

- These results are often obtained in controlled environments
- External validity remains limited

7. Contribution of the study

This study contributes to:

- ☐ understanding trends in AI in cybersecurity
- ☐ identifying the most effective techniques
- ☐ guiding future research

8. Overall limitations of the study

- ☐ **External validity:** Data often unrealistic
- ☐ **Scalability:** Difficulty of application on a large scale
- ☐ **Human factor:** Not taken into account

9. Positioning in relation to my project

My project improves this study by:

- ✓ integrating Zero Trust
- ✓ adding cyber resilience
- ✓ proposing a real experimental model
- ✓ adapting to resource-constrained environments

Conclusion

In conclusion,

This study demonstrates the importance of artificial intelligence in cybersecurity.

However, it has significant limitations related to:

- the lack of complete theoretical integration
- the lack of experimentation
- the low consideration of the human factor

My project aims to fill these gaps by proposing an integrated approach
thank you for your attention.

Key References (APA)

Zhang, Y., Chen, X., Li, L., & Wong, D. S. (2022). Artificial intelligence in cloud security: A survey. *IEEE Access*, 10, 53487–53506.
<https://doi.org/10.1109/ACCESS.2022.3171803>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

