



Literary Criticism (3) _Task 3
**Analyze the methodology, examine
the statistical methods, and assess
their suitability for the research
objectives.**

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 3

Introduction

Assalamu Alaikum,
Peace be upon you.

As part of the Literary Criticism 3 course at Midocean University, I am presenting today the assignment for the third week.

The task consists of:

- ❖ Choosing a thesis topic in my field of specialization,
- ❖ Analyzing the methodology used,
- ❖ Examining the statistical methods,
- ❖ And evaluating their suitability for the research objectives.

1. Thesis topic selection (New trend in cybersecurity)

I have chosen a recent thesis entitled:

“Artificial Intelligence–Driven Zero Trust Architecture for Cloud Security Resilience”

Author: Emily Carter

University: University College London

Year: 2023

PhD in Cybersecurity Engineering

This choice is relevant because it addresses two major trends:

- ☐ The integration of Artificial Intelligence in cybersecurity
- ☐ The Zero Trust architecture applied to Cloud environments

These topics today represent a strategic evolution in response to advanced threats.

2. Research objectives

The study has three main objectives:

- Design an AI-based Zero Trust model.
 - Measure its effectiveness against advanced persistent threats.
 - Compare its performance to traditional perimeter security models.
- These objectives combine conceptual, experimental, and comparative aspects.

3. Analysis of the methodology

The author adopts a mixed experimental and quantitative methodology.

The research includes:

- ☐ A phase of theoretical model design
- ☐ A simulation in a Cloud environment
- ☐ A controlled experiment
- ☐ A statistical analysis of the results

Unlike the previous study, here the triangulation is clearly sequential:

Step 1: Theoretical design

Step 2: Experimental implementation

Step 3: Statistical validation

Step 4: Inter-model comparison

Each step builds on the previous one.

This strengthens:

- ❖ Internal validity
- ❖ Logical consistency
- ❖ Scientific reproducibility

4. Statistical methods used

The study uses several advanced statistical tools:

1. Analysis of Variance (ANOVA)
2. Student's t-test
3. Logistic regression
4. Measurement of the detection rate (True Positive Rate)
5. ROC analysis (Receiver Operating Characteristic)

Why these methods?

- ☐ ANOVA allows for the comparison of several security configurations.
- ☐ The t-test assesses significant differences between two architectures.
- ☐ Logistic regression models the probability of attack detection.
- ☐ The ROC curve measures the AI model's performance.

5. Assessment of methodology suitability – objectives

Objective 1: Design a model

The conceptual phase is consistent with an experimental approach.

Objective 2: Measure effectiveness

The use of quantitative metrics and statistical analyses is perfectly aligned with this objective. Statistical tests allow the performance to be scientifically demonstrated.

Objective 3: Comparison

ANOVA and comparative tests directly support this objective.

There is therefore strong internal consistency between:

- ☐ The announced objectives
- ☐ The methodological tools
- ☐ The statistical methods used

6. Personal critical analysis

Despite this rigor, I identify certain limitations:

- ◆ The experimentation is carried out in a simulated, not real, environment.
- ◆ The data used come from public Western databases.
- ◆ The study does not test the model in developing country contexts.

Thus, although the internal validity is strong, the external validity could be improved. An extension to real critical infrastructures would strengthen the robustness.

CONCLUSION

In conclusion,

This thesis represents a significant contribution to emerging trends in cybersecurity, notably:

- ❖ **The integration of AI**
- ❖ **The Zero Trust architecture**
- ❖ **Advanced statistical analysis**

The methodology is sequential, coherent, and well-aligned with the objectives.

The statistical methods are relevant and suitable for the hypotheses.

However, diversification of experimental contexts would improve the generalizability of the results.

This analysis demonstrates the importance of evaluating not only technical robustness but also methodological and contextual appropriateness in any doctoral research.

Thank you for your attention.

Assalamu Alaikum. رمضان مبارك

- 1) Here are the key academic references supporting I selected thesis topic on: Artificial Intelligence–Driven Zero Trust Architecture for Cloud Security Resilience (2023). These references cover Zero Trust, AI in cybersecurity, Cloud security, and statistical evaluation methods.
- 2) 2) Zero Trust Architecture
National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture (SP 800-207). Gaithersburg, MD: NIST.
Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207.
- 3) Artificial Intelligence in Cybersecurity
IEEE (2021). Artificial Intelligence in Cybersecurity. IEEE Security & Privacy Journal.
Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.
Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Commun
- 4) Statistical & Experimental Validation Methods
Montgomery, D. C. (2019).
Design and Analysis of Experiments (10th ed.). Wiley.
Experimental design.
Fawcett, T. (2006).
An Introduction to ROC Analysis.
Pattern Recognition Letters, 27(8), 861–874.....



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

