



**Analyze the study results and
check their relationship with the
research hypotheses.**

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 4

Introduction

Assalamu Alaikum,
May peace be upon you.

As part of the Literary Criticism 3 course, today I am presenting a critical analysis of the results of a doctoral study in cybersecurity, as well as an evaluation of their relationship with the research hypotheses.

The chosen study is a recent thesis entitled:

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

This research falls within the new trends in cybersecurity, notably:

- ❑ **the integration of artificial intelligence in attack detection,**
- ❑ **Zero Trust architecture applied to cloud environments.**

The conceptual framework of this architecture is based in particular on the recommendations of the National Institute of Standards and Technology (NIST) regarding Zero Trust models.

1) Research questions

Before analyzing the results, it is important to present the research questions, as they guide the entire methodology and analysis of the results.

The study is based on three main questions:

RQ1:

Does the AI-based Zero Trust architecture improve the detection of cyberattacks in cloud environments?

RQ2:

Is the proposed model more effective than traditional perimeter security models?

RQ3:

Does the integration of artificial intelligence reduce the false positive rate in intrusion detection systems?

These questions structure the entire experimentation.

2. Research hypotheses

From these questions, the author formulates the following hypotheses:

H1:

The AI-based Zero Trust model significantly improves the attack detection rate.

H2:

The proposed model offers better performance than traditional security architectures.

H3:

The integration of artificial intelligence reduces false positives in intrusion detection.

These hypotheses were then tested through simulated experiments.

3. Experimental environment

The study was conducted in a simulation environment using:

- the CloudSim platform to simulate a cloud infrastructure, attack
- databases such as CICIDS2017,
- and an intrusion detection system based on machine learning. The

models compared in the study are:

1. Traditional perimeter security model,
2. Classic Zero Trust architecture,
3. AI-based Zero Trust architecture proposed by the author.

This comparison allows for an objective evaluation of the performance of the new model.

4. Main results of the study

The results obtained show that:

- ❑ The AI-based Zero Trust model reaches a detection rate of 96%,
- ❑ The classic Zero Trust architecture reaches about 89%,
The traditional perimeter model reaches only 82%.

Regarding false positives:

-The proposed model reduces the false positive rate by 18% compared to traditional systems.

These results indicate a significant improvement in performance.

Statistical methods used to validate the results

To verify the scientific validity of the results, the author uses several statistical methods.

ANOVA Analysis

Analysis of variance (ANOVA) is used to compare the performance of the three security models. This method allows determining if the observed differences are statistically significant. The results show a significant difference between the models.

Student t-test

After the ANOVA, the author uses a t-test to compare more precisely:
the classic Zero Trust model
and the AI-based Zero Trust model.

The t-test is necessary here to perform a pairwise comparison between two specific architectures.

The results indicate that the improvement of the proposed model is statistically significant

Critical analysis of the results–hypotheses relationship

The results obtained generally confirm the hypotheses of the study.

Hypothesis H1

The improvement in the detection rate confirms that the integration of artificial intelligence enhances the system's efficiency.

Hypothesis H2

The comparison with traditional models demonstrates that the proposed architecture is more efficient.

Hypothesis H3

The reduction in false positives also confirms the effectiveness of the machine learning model.

Thus, the results clearly support the formulated hypotheses.

Personal critical analysis

Despite these promising results, certain limitations must be mentioned.

First, the experiments were conducted in a simulated environment and not in a real cloud infrastructure.

Second, the data used mainly come from experimental databases.

Third, the study does not test the architecture in real critical infrastructures such as energy or industrial networks.

These factors may limit the **external validity** of the results.

CONCLUSION

In conclusion, this study demonstrates that the integration of artificial intelligence into a Zero Trust architecture can significantly improve the security of cloud environments.

The experimental results confirm the research hypotheses and show a notable improvement in the cyberattack detection rate.

However, additional validations in real environments would be necessary to confirm the model's applicability in critical infrastructures.

Thank you for your attention.

Assalamu Alaikum. رمضان مبارك

- 1) National Institute of Standards and Technology. (2020).
Rose, S., Borchert, O., Mitchell, S., & Connelly, S.
Zero Trust Architecture (NIST Special Publication 800-207).
Gaithersburg, MD: NIST.
- 2) Kindervag, J. (2010).
Build Security Into Your Network's DNA: The Zero Trust Network Architecture.
Forrester Research
- 3) Buczak, A. L., & Guven, E. (2016).
A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.
IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
- 4) Sommer, R., & Paxson, V. (2010).
Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.
Proceedings of the IEEE Symposium on Security and Privacy.
- 5) IEEE. (2021).
Artificial Intelligence and Machine Learning for Cybersecurity.
IEEE Security & Privacy Journal.
- 6) Cloud Security Alliance. (2022). Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0).
Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A Survey of Intrusion Detection Techniques in Cloud.
Journal of Network and Computer Applications, 36(1), 42–57



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

