



The context of task 5: presenting observations, recommendations, and proposals for future research

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 5

Introduction

السلام عليكم

As part of the course Midocean University – Literary Criticism 3, I am presenting today the fifth task, which consists of analyzing a thesis in my field of specialization, making critical observations, and proposing recommendations to improve the study as well as avenues for future research.

The study analyzed is the thesis entitled:

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

Author: Emily Carter

University: University College London

Year of Publication: 2023

This research focuses on the use of artificial intelligence to enhance Zero Trust architectures in cloud environments.

The conceptual framework of the study is based in particular on the security principles developed by the National Institute of Standards and Technology, which defines modern Zero Trust architecture models.

1) General overview of the study

The main objective of this research is to develop a cybersecurity architecture based on:

- ❑ artificial intelligence
- ❑ The Zero Trust model

The protection of cloud infrastructures against advanced cyberattacks.

The study proposes a model capable of improving attack detection and reducing false positives in security systems.

To test this model, the author uses:

- ❖ a cloud simulation environment
- ❖ machine learning algorithms
- ❖ statistical methods to validate the results.

2. Critical observations on the study

Despite the significant contributions of this research, several critical observations can be made.

First, the study relies mainly on a simulated environment.

Although simulations are useful for testing experimental models, they do not always reflect the real conditions of complex cloud infrastructures.

Second, the data used to train the artificial intelligence models come from public databases, which may limit the diversity of the attack scenarios studied.

Third, the study focuses mainly on the technical aspects of the model and pays less attention to organizational and human factors, which nevertheless play an important role in cybersecurity.

3. Recommendations to improve the study

To strengthen the scientific quality of this research, several improvements could be considered.

Firstly, it would be relevant to test the proposed architecture in a real cloud environment, for example in company infrastructures or data centers.

Secondly, the study could incorporate more varied datasets, including real attack scenarios from different industrial sectors.

Thirdly, the author could integrate a multidisciplinary approach by including organizational factors, such as security policy management and user training.

These improvements would increase the external validity and practical applicability of the proposed model.

4. Proposals for future research

Based on the limitations identified in this study, several directions for future research can be proposed.

A first avenue is to study the integration of artificial intelligence into Zero Trust architectures for the protection of critical infrastructures, such as energy networks or financial systems.

A second avenue would be to explore the use of federated learning, which allows training artificial intelligence models without directly sharing sensitive data.

Finally, future research could analyze how Zero Trust architectures can be adapted to developing countries, where technological resources and cybersecurity capabilities are sometimes limited.

CONCLUSION

In conclusion, this thesis makes an important contribution to the new trends in cybersecurity, notably through the integration of artificial intelligence into Zero Trust architectures for cloud environments.

However, certain limitations related to the experimental environment and the data used suggest the need for further studies.

The recommendations and research avenues proposed could help improve the robustness and applicability of this type of cybersecurity solutions in real-world environments.

Thank you for your attention.

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. IEEE. (2021).
- 5) Cloud Security Alliance. (2022).
Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0).
- 6) Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013).
A Survey of Intrusion Detection Techniques in Cloud Computing.
Journal of Network and Computer Applications, 36(1), 42–57
- 7) **Creswell, J. W., & Creswell, J. D. (2018).**
Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.).
Sage Publications.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

