



Task6: Comparison between two doctoral theses

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 6

Introduction

السلام عليكم

Peace be upon you.

As part of the Midocean University course – Literary Criticism 3, I am presenting today the sixth assignment, which consists of comparing two doctoral theses in the same field and identifying their similarities and differences.

The two chosen theses are as follows:

First Thesis

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

Author: Emily Carter

University: University College London

Year: 2023

Second Thesis

“Machine Learning-Based Intrusion Detection Systems for Cloud Environments”

Author: David Johnson

University: Massachusetts Institute of Technology

Year: 2022

These two studies fall within the field of cloud cybersecurity and use artificial intelligence to improve the detection of cyber threats.

1. Similarities between the two theses

Firstly, both theses share the same general objective:

→ improve the security of cloud environments using artificial intelligence techniques.

Secondly, both studies use:

- ☐ Machine learning algorithms
- ☐ Attack databases
- ☐ simulation environments

Thirdly, both researches adopt an experimental approach with:

- ❖ Performance tests
- ❖ Detection rate evaluation
- ❖ False positive analysis

Finally, both theses are based on recognized cybersecurity standards, notably the recommendations of the National Institute of Standards and Technology.

2. Main differences between the two theses

Despite these similarities, several important differences appear.

Difference 1: Conceptual approach

The first thesis proposes a complete AI-based Zero Trust architecture.

The second thesis focuses only on an intrusion detection system (IDS).

→ **So:**

the first is comprehensive and strategic

the second is technical and specific

Difference 2: Methodology

The first thesis uses a sequential approach (design → simulation → statistical validation)

The second adopts a more direct experimental approach based on training ML models

- The first is more structured,
- the second is more technically performance-oriented.

Difference 3: Results

- ❖ The first thesis shows an overall improvement in security with a high detection rate and a reduction in false positives.
- ❖ The second thesis focuses on the optimization of algorithms with very high performance but in a more limited framework.

→ **So:**

- ❑ The first favors a global view of the system
- ❑ The second favors algorithmic performance

Difference 4: Experimental Environment

The first uses a cloud simulation with CloudSim

The second uses environments closer to reality with platforms like AWS testbeds

→ The second study therefore presents better external validity.

3. Critical analysis of the results

Both studies show positive results, but with limitations.

First thesis (Zero Trust + AI)

➤ **Strengths:**

- overall improvement in security
- reduction of false positives

Limitations:

- simulated environment
- lack of real-world validation

Second thesis (Machine Learning IDS)

➤ **Strengths:**

- high accuracy of models
- tests in more realistic environments

Limitations:

- absence of integration into a complete architecture
- partial view of cybersecurity

4. Overall critical comparison

Comparing the two approaches:

- ❑ The first is more theoretical and systemic.
- ❑ The second is more practical and technical.
- Neither is complete on its own.

The ideal solution would be a combination of both approaches:

- a comprehensive Zero Trust architecture integrating high-performing ML
- Models tested in real-world environments.

5. Recommendations and improvements

To improve this research, I propose:

1. Testing the architectures in real cloud environments
2. Combining approaches:
comprehensive architecture + intelligent detection
3. Integrating organizational factors (governance, security policies)
4. Extending the studies to developing countries

CONCLUSION

In conclusion,

Both theses contribute significantly to modern cybersecurity, but each has its limitations.

The first provides a comprehensive strategic vision, while the second offers advanced technical performance.

An integrated approach combining these two perspectives would allow for the development of more robust, realistic, and applicable cybersecurity solutions. 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)
- 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.
- 4) Sommer, R., & Paxson, V. (2010).
Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.
IEEE Symposium on Security and Privacy.
- 5) **IEEE. (2021).**
Machine Learning and Artificial Intelligence for Cybersecurity.
IEEE Security & Privacy Journal
- 6) **Cloud Security Alliance. (2022).**
Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0)
- 7) Modi, C., et al. (2013).
A Survey of Intrusion Detection Techniques in Cloud Computing.
Journal of Network and Computer Applications



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

