



Task 7 – Critique of the Research Methodology

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 7

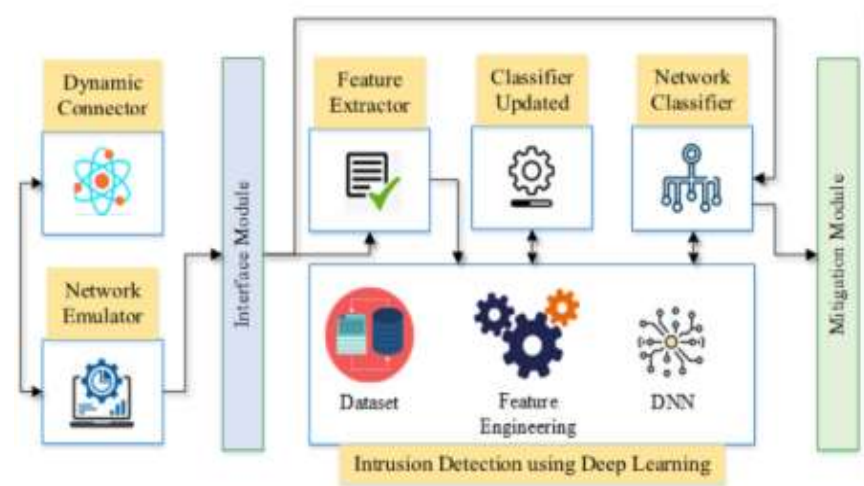
INTRODUCTION

Hello everyone,
I am Ali Mmadi, a PhD student in Information Technology, specializing in Cybersecurity.

In this seventh task of the Critical Studies 2 module, I will analyze and evaluate the research methodology used in a scientific article entitled:

“Machine Learning-Based Intrusion Detection in IoT Networks: A Comparative Performance Evaluation,” published in IEEE Access in 2022.

The aim of this critique is to determine whether the chosen methodology is appropriate, scientifically sound, and consistent with the study's objectives.



1) Relevance of the methodological choice

Critical analysis:

✓ The choice of a quantitative methodology is perfectly appropriate, as the subject deals with algorithm performance, which requires numerical measurements:

- accuracy
- recall
- F1-score
- false positive rate

Area for improvement:

The authors did not explain why they chose an **exclusively quantitative** approach, and did not consider a mixed method incorporating **interviews with IoT administrators**, which would have added an additional contextual dimension.

2) Relevance of data collection tools

The researchers used:

❑ **a public dataset:**

NSL-KDD + a synthetic IoT dataset,

❑ **machine learning tools:** *Python, Scikit-Learn, TensorFlow.*

Critical Analysis:

The chosen datasets are relevant for studying an intrusion detection system.
They allow for obtaining balanced and varied data.

⚠ Methodological limitation:

The study does not sufficiently justify the choice of the synthetic IoT dataset.
A real dataset, collected in an actual IoT environment, would have strengthened the **external validity** of the research.

3) Description of the population, the sample, and the procedures

Since this is an experimental quantitative study, the "population" corresponds to IoT network traffic.

The sample used includes:

125,000 normal network packets

35,000 malicious packets including botnet, DDoS, reconnaissance, and injection.

Critical analysis:

✓ The sample size is sufficiently large, allowing for reliable statistical tests.

⚠ However, the description lacks essential details:

Which IoT protocol (MQTT? CoAP?)

What network structure was used?

What was the time period of data capture?

These elements are important to verify the reproducibility of the research.

4) Relevance and sample size

The sample size is generally satisfactory. It allows for effective testing of algorithms such as Random Forest, SVM, CNN, or LSTM.

Critical analysis:

□ However, the authors do not explain whether the sample was balanced or if they addressed class imbalance issues, which are very common in cybersecurity.

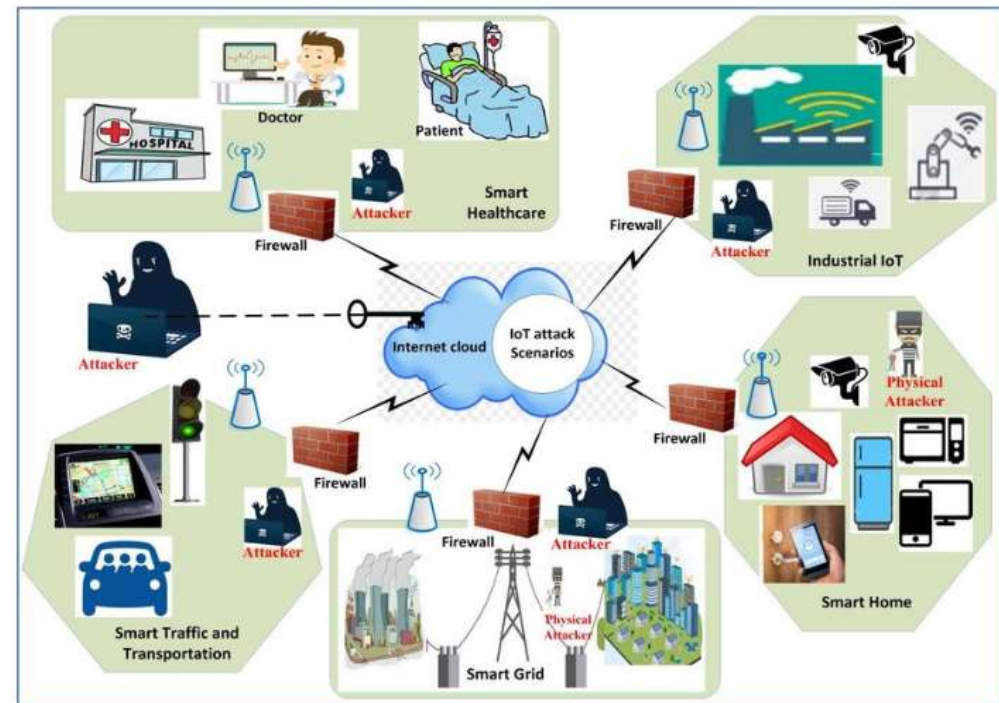
Without this information, it is difficult to assess the **robustness** of the model.

5) Sample characteristics

The types of attacks are relevant for an IoT network, but:

⚠ The study omits some types of modern threats, such as:

- IoT deepfake attack firmware
- manipulation attacks on the radio layer
- This slightly limits the practical scope of the research.



6. Use of statistical software and models

The authors mention having used:

- ☐ Python (NumPy, Pandas)
- ☐ Scikit-Learn
- ☐ TensorFlow
- ☐ and standard performance metrics.



Critical analysis:

- ✓ The software is suitable for quantitative analysis in cybersecurity.
- ✓ The statistical metrics are relevant.
- ✗ However, the authors do not explain how the hyperparameters were chosen,
- ✗ nor whether they performed cross-validation.

Without these details, the credibility of the results is less solid.

CONCLUSION

In conclusion, the study's methodology is overall appropriate, coherent, and scientifically sound.

The choice of a quantitative method is justified to measure the performance of the models, and the data collection tools are relevant.

However, several improvements can be made:

- explain the choice of datasets,
- detail the model parameters,
- specify the full characteristics of the sample,
- and strengthen the justification of the experimental protocol.

This critique shows that a good study in cybersecurity relies on a clear, justified, and rigorous methodology.

Thank you for your attention.

- 1) Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2022).
Machine Learning-Based Intrusion Detection in IoT Networks: A Comparative Performance Evaluation.
IEEE Access, 10, 10355–10368.
(Main study used for Task 7)
◆ Machine Learning for Intrusion Detection
- 2) Khan, M. A., & Salah, K. (2018).
IoT Security: Review, Blockchain Solutions, and Open Challenges.
Future Generation Computer Systems, 82, 395–411.
- 3) Fernandes, E. et al. (2017).
Flow-Based Anomaly Detection in IoT Networks Using Machine Learning.
2017 IEEE Symposium on Computers and Communication.
- 4) Liu, H., Lang, B., & Liu, M. (2019).
A Comparative Study of Machine Learning Algorithms for Network Intrusion Detection.
Computers & Security, 88, 101636.
◆ IoT Cybersecurity Frameworks & Threats
- 5) Sfar, A. R., Natalizio, E., Chowdhury, N., & Francesca, S. (2018).
A Roadmap for Security Challenges in the Internet of Things.
Digital Communications and Networks, 4(2), 118–137.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

