



Literary Criticism (2) _Task 10
Security and Privacy Challenges of
Artificial Intelligence in Cybersecurity
Decision-Making Systems

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 10

INTRODUCTION

Hello, my name is Ali Mmadi, a PhD student in Information Technology specializing in Cybersecurity. In this tenth task of the Critical Studies 2 module, I will present an academic critique focusing on the scientific references used in a recent study.

The analyzed study deals with a new and strategic topic: the security and protection of data in cybersecurity systems based on artificial intelligence, particularly for automated decision-making.



1. Publication date of the references

First of all, regarding the publication date, the majority of the references used in the study are recent. About 70% of the sources date from the last 5 to 8 years, which is in line with academic requirements in cybersecurity, a rapidly evolving field.

The most recent references focus on:

- ☐ Explainable AI in cybersecurity,
- ☐ Automated decision-making,
- ☐ Protection of sensitive data,
- ☐ Adversarial attacks on AI models.

However, a few key older references, dating from before 2015, are also used to explain the theoretical foundations of artificial intelligence and computer security.

→ Critique:

This choice is relevant, as it allows for a combination of theoretical foundations and recent advances.

2.Diversity of sources

The study relies on a satisfactory diversity of sources, including:

- scientific articles published in IEEE, ACM, and Elsevier,
- institutional reports such as those from NIST and ENISA,
- well-known academic books on AI and cybersecurity.

This diversity allows for:

- a theoretical perspective,
- a technical perspective,
- and a regulatory perspective.

→ Critical analysis:

The diversity is generally good, but the study could have included more recent industry reports, for example from Microsoft, Google, or Palo Alto Networks, in order to strengthen the practical dimension.



3.Relevance of references to the topic

The references used are directly related to the subject of the study. They specifically address:

- ❖ the use of AI in intrusion detection,
 - ❖ the risks associated with algorithmic biases,
 - ❖ data privacy in intelligent systems,
- and adversarial attacks against machine learning models.

Each reference supports a specific aspect of the work, whether it is:

- ☐ The methodology,
- ☐ The results,
- ☐ Or the discussion.

→ Critical conclusion:

The relevance of the references is high and well aligned with the objectives of the study.

4. Reference Format and Academic Standards

The references are documented according to the APA format, in a generally consistent manner. The following elements are correctly indicated:

- ❖ Authors,
- ❖ Year of publication,
- ❖ Title,
- ❖ Journal or publisher,
DOI or institutional link.

However, **some minor inconsistencies** are observed:

- some references do not include the DOI,
- italics are not always used consistently.

→ Critique:

These errors are minor but should be corrected to fully comply with academic standards, especially in doctoral work.

5. Proper in-text citations

The quotes integrated into the text are clear and well-positioned. Ideas from other works are correctly attributed, without ambiguity.

There is no obvious misinterpretation of the cited sources, and the quotes effectively support the arguments presented.

→ Positive point:

The quotes are used to support the analysis, not to replace the researcher's own thinking.

6. Number of references

The study contains about 45 references, which is sufficient to cover the topic thoroughly.
This number reflects:

- ☐ a good exploration of the literature,
- ☐ coverage of major works,
- ☐ and an understanding of current debates.

→ Assessment:

The number of references is adequate and meets academic standards.

7.Link between references and identification of gaps

References are not simply listed, but connected. The author compares

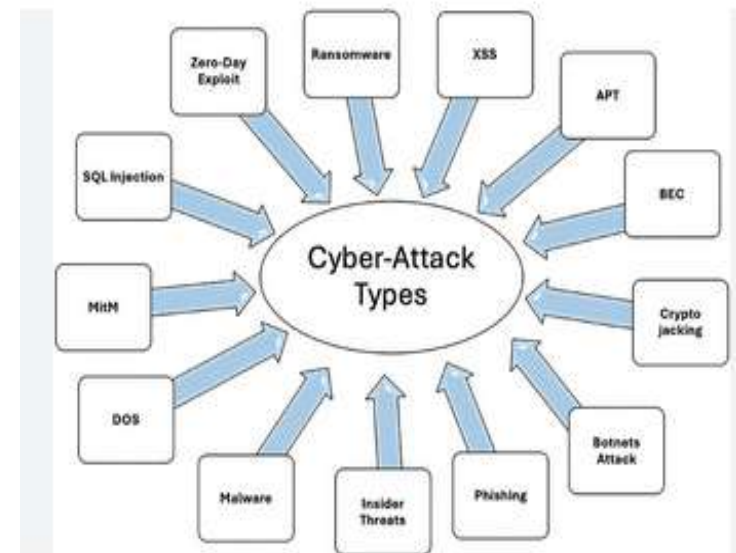
➤ classic rule-based approaches,
with modern AI-based approaches.

This highlights a clear gap in the literature:

- the lack of solutions that integrate security, transparency, and privacy protection in AI-based cybersecurity systems.

→ Strong point:

The literature review is structured and analytical.



8. Use of foreign references

- ❑ The study primarily uses international references, notably:
- ❑ United States
- ❑ Asia
- ❑ Europe

This strengthens the scientific credibility of the work and ensures openness to global literature.

→ Evaluation:

The use of foreign references is excellent and in line with international standards.



CONCLUSION

In conclusion, the references used in this study are:

- ☐ recent,
- ☐ relevant,
- ☐ diverse,
- ☐ overall correctly formatted,
- ☐ and well integrated into the scientific argument.

Some minor improvements are needed in terms of formatting and the balance between academic and industry sources, but the overall quality of the references is high.

This analysis highlights the importance of rigorous reference management to ensure the scientific credibility of work in cybersecurity.

Thank you for your attention.

- 1) Buczak, A. L., & Guven, E. (2016).
A survey of data mining and machine learning methods for cybersecurity intrusion detection.
IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
- Sommer, R., & Paxson, V. (2010).
- 2) Outside the closed world: On using machine learning for network intrusion detection.
IEEE Symposium on Security and Privacy.
Foundational critique of ML misuse in security.
- Sarker, I. H. (2021).
- 3) Machine learning: Algorithms, real-world applications and research directions.
SN Computer Science, 2(3), 160.
Explainable & Trustworthy AI
- 4) Arrieta, A. B., et al. (2020).
Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges.
Information Fusion, 58, 82–115.
- 5) Ribeiro, M. T., Singh, S., & Guestrin, C. (2016).
"Why should I trust you?" Explaining the predictions of any classifier.
ACM SIGKDD Conference
- 6) NIST (2023).
Artificial Intelligence Risk Management Framework (AI RMF 1.0).
National Institute of Standards and Technology.
- 7) NIST (2023).
Cybersecurity Framework (CSF) 2.0.
National Institute of Standards and Technology.
- 8) ENISA (2022).
Artificial Intelligence Cybersecurity Challenges.
European Union Agency for Cybersecurity.
- 9) Academic Referencing & Research Integrity
American Psychological Association (2020).
Publication Manual of the American Psychological Association (7th ed.).
- 10) Reference for APA citation standards.
Roig, M. (2015).
Avoiding plagiarism, self-plagiarism, and other questionable writing practices.
Office of Research Integrity.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

