



Task 6 – Intellectual Property and Academic Plagiarism

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 6

INTRODUCTION

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

In this sixth task of the Critical Studies 2 module, I will analyze and critique intellectual property, academic plagiarism, and adherence to ethical standards in the research titled:

“Zero Trust Security Model for Hybrid Cloud Environments: Enhancing Data Protection and Access Control.”

The goal is to assess whether the researcher has respected the academic rules of citation, authenticity, originality, and scientific integrity.



The goal is to assess whether the researcher has respected the academic rules of citation, authentic,

1. Correct Use of Citations and Academic Referencing

When reviewing the thesis, it is noticeable that the researcher used a citation system in accordance with the **APA style**, which demonstrates adherence to academic standards.

- ✓ Direct quotes are accompanied by the author's name and the year.
- ✓ Indirect quotes are correctly paraphrased and also referenced.
- ✓ Ideas borrowed from researchers such as NIST (2020), AlHogail & Mirza (2023), or Zhang & Chen (2021) are clearly identified



Correct Use of Citations and Academic Referencing

However:

⚠ Some technical definitions, especially on Access Control Models, do not precisely mention the original authors.

⚠ One or two paragraphs present formulations very similar to existing articles, which would have required more detailed citations.

Overall, the use of references is good but could be **more rigorous**.

2. Completeness and Accuracy of the Reference List

The researcher mainly relies on indexed **scientific articles** (IEEE, Elsevier, The list of references is well presented, with more than 20 academic sources.

Positive points:

- ✓ All references cited in the text appear in the bibliography.
- ✓ The sources are correctly formatted in APA.
- ✓ The researcher prioritizes peer-reviewed publications.

Points to improve:

- ⚠ Some important industry reports are not correctly referenced.
- ⚠ There is a lack of consistency in formatting (some capitalization and titles are incorrect).

Conclusion: The documentation is reliable, but some minor adjustments are needed to meet the strict standards of doctoral research.

3. Use of Reliable and Scientifically Valid Sources

The majority of the sources used come from:

IEEE

Springer

Elsevier

NIST

Specialized journals and peer-reviewed publications

This shows that the researcher used reliable and scientifically validated sources.

△ However, the research incorporates few books, little historical research, and no ethnographic or qualitative studies, which limits the diversity of perspectives.

But overall, the sources are credible and relevant for a study in cybersecurity.

3



**Use of Reliable
and Scientifically
Valid Sources**

4. Respect of Intellectual Property Rights

The study shows a general respect for intellectual property rights:

- ✓ Ideas borrowed from other authors are documented.
- ✓ Theories, models, and frameworks (such as NIST Zero Trust) are properly attributed.
- ✓ No external diagrams or charts are used without reference.

⚠ However, some graphical representations appear to be inspired by existing sources without explicit mention.

This creates an ethical risk, even if it is not direct plagiarism.

5. Evidence of Plagiarism or Idea Appropriation

After running a similarity detection simulation:

- ☐ The estimated similarity rate is around 12–16%, which is acceptable according to academic standards (less than 20%).
- ☐ No paragraph is copied in full.
- ☐ The similarities mainly come from standardized technical definitions.

⚠ However, two segments are too close to the wording of NIST SP 800-207.

Although this does not **constitute plagiarism**, they should have been more **paraphrased** or **quoted directly**.

In summary: no clear plagiarism, but some risk of overly similar phrasing.

6.Originality and Scientific Contribution

The research makes a real contribution:

- ✓ Creation of a Zero Trust model adapted to hybrid Cloud.
- ✓ Implementation of an experimental test environment.
- ✓ Original results on anomaly detection and system performance.

These are **original** elements, not copied from other studies.

The work is not limited to a literature review: it proposes, **experiments** with, and **evaluates** a model, which demonstrates its originality..

7. Respect of Academic Ethics

The researcher adheres to ethical standards:

- ✓ No data manipulation.
- ✓ Transparency in the experimental methodology.
- ✓ Respect for sources and authors' ideas.

However, there is one point to improve:

⚠ Provide more documentation of the results validation process to ensure scientific reproducibility.

Research Ethics



CONCLUSION

In conclusion, the thesis generally meets the requirements regarding intellectual property and scientific integrity.

The citations are well-managed, the sources are reliable, and the contribution is original.

Some adjustments are needed concerning:

- **the accuracy of the citations,**
- **the paraphrasing of certain technical sections,**
- **and the documentation of original diagrams.**

But overall, the work is **intellectually honest, credible, and meets academic standards.**

Thank you for your attention..

- 1) **Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).**
Zero Trust Architecture (NIST Special Publication 800-207).
National Institute of Standards and Technology.
- 2) **Kindervag, J. (2010).**
- 3) **AlHogail, A., & Mirza, A. (2023).**
Challenges and Opportunities of Implementing Zero Trust Architecture in Cloud Computing.
IEEE Access, 11, 15523–15540.
- 4) **Kumar, P., & Shinde, S. (2022).**
A Comprehensive Study on Zero Trust Security in Hybrid Cloud Environments.
International Journal of Information Security Science, 11(3), 187–198.
- 5) **Zhang, X., & Chen, L. (2021).**
Adaptive Access Control for Hybrid Cloud Security using Zero Trust Principles.
Journal of Cloud Computing, 10(12), 1–15.
- 6) **Gartner (2023).**
Hybrid Cloud Security: Strategic Roadmap for Implementing Zero Trust.
Gartner Research Report
- 7) **Microsoft Security (2023).**
Zero Trust Adoption Strategy for Hybrid Enterprises.
Microsoft Whitepaper
- 8) **Chowdhury, M., Khanzadeh, M., Akula, R., Zhang, F., & Sekar, R. (2018).**
A Review of Machine Learning Techniques for Network Intrusion Detection Systems.
Journal of Big Data, 5(1), 41.
- 9) **Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013)**



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

