

Academic critique of the problem and the significance of the research message

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 3

INTRODUCTION

Hello everyone,

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

In this third assignment of the Critical Studies 2 module, I will present an academic critique of the problem and the significance of the research message, based on an actual Master's thesis entitled:

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

This thesis was defended at the University of Twente (Netherlands, 2023).

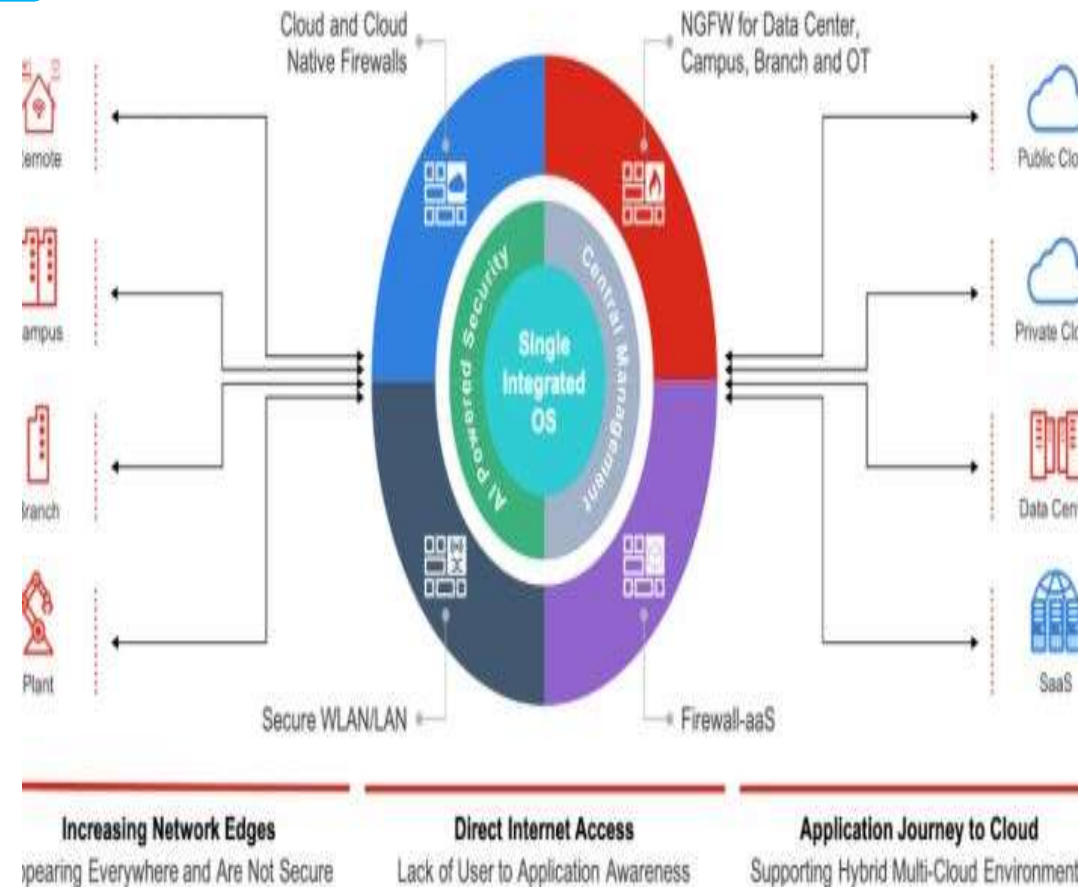
1. Definition of the research problem

The researcher clearly defines the topic from the first paragraph: he introduces the concept of Zero Trust as a necessary evolution in response to the obsolescence of the traditional perimeter model.

However, the problem of the thesis is not formulated in a sufficiently concise manner. He mentions the growth of hybrid Cloud and the associated risks, but the research question could have been expressed in a more direct form, for example:

"How can an effective Zero Trust framework be designed to secure interactions between on-premises and public Cloud environments?"

In other words, the introduction presents the general theme well, but the precise formulation of the scientific problem remains somewhat diffuse.



2. Critique: Does the problem reflect a real significance?

Yes, the issue is highly relevant and topical. Cyberattacks on hybrid Cloud environments have increased with the widespread adoption of remote work and migration to the Cloud. Reports from Gartner (2024) and IBM Security (2023) confirm that over 60% of Cloud data breaches stem from poor management of internal trust.

This problem therefore deserves a **thorough analysis**, as it directly affects **organizational security, access policies**, and the protection of sensitive data.

However, it is noted that the researcher could have **strengthened the importance** of the problem by citing recent statistics or examples of concrete attacks (for instance, the attacks on Microsoft Exchange Cloud or Capital One Cloud in 2019).

This would have helped support the severity of the problem with **solid empirical** evidence.

3. Link with practical and scientific context

The problem is directly related to the context of the research, as it falls within the digital transition of companies.

The Zero Trust model, the central focus of the research, is a practical and conceptual response to this reality:

“Never trust, always verify.”

This link between theory and practice makes the issue relevant both for the **scientific community** and for **cybersecurity professionals**.

→ However, the researcher did not clearly specify **the sectoral scope** (for example, industrial companies, public institutions, etc.), which limits the practical applicability of the study.

4. Definition of the dimensions of the problem

Regarding the temporal, geographical, and technical dimensions, the research briefly mentions that the study focuses on recent hybrid Cloud infrastructures (post-2020). However:

- ❑ There is no **clear geographical delimitation** (region, continent, type of company).
- ❑ **The target population** (administrators, CIOs, Cloud providers) is not explicitly defined.
- This lack of precision limits the **generalizability** of the results.

5. Presence of a gap in the literature

The researcher correctly identified a **gap**: few studies incorporate **Zero Trust** in hybrid Cloud contexts with quantitative approaches.

He points out that the majority of previous work remains **conceptual** or focused on public Cloud environments.

✓ This observation is accurate and supported by literature reviews (e.g., IEEE Access, 2022).

However, the researcher did not utilize a **critical comparison** between existing models

(NIST Zero Trust Framework, Google BeyondCorp, etc.), which would have better positioned his contribution.

6. Final assessment by the critic

In summary:

- ❑ The problem is well-chosen, clear, and relevant, addressing a real need in the field of cybersecurity.
- ❑ The link to practical reality is strong but could benefit from more contextual precision.
- ❑ The dimensions of the problem are mentioned but not sufficiently defined.
- ❑ The scientific gap is identified but lacks comparative grounding with other models. Thus, I consider that the researcher **has formulated the problem well** but **needs to strengthen the analytical depth and contextual precision** to meet the standards of advanced scientific research.

CONCLUSION

In conclusion, this review demonstrates that in the field of cybersecurity, the quality of a research problem depends not only on its relevance, but also on:

the clarity of its scope,
the presence of empirical evidence,
and the scientific justification of the identified gap.

Thank you for your attention.

I am Ali Mmadi, a PhD student in Information Technology and Cybersecurity.

- [1] J. K. Martin, « Nuages hybrides : le meilleur des deux mondes ? », IEEE Cloud Computing, vol. 2, no 3, pp. 24-30, 2015.
- [2] A. Kindervag, Zero Trust Networks : Construire des systèmes sécurisés dans des réseaux non fiables, O'Reilly Media, Inc., 2017.
- [3] S. Gallagher, et M. B. Friksen, « Architecture Zero Trust : Aperçu et évaluation », IEEE Security & Privacy, vol. 18, no 3, pp. 42-49, 2020.
- [4] Cong Wang et al., « Vers des services de stockage sécurisés et fiables dans le cloud computing », IEEE Transactions on Services Computing, vol. 5, no 2, pp. 220-232, 2012. [CrossRef] [Google Scholar] [Lien de l'éditeur]
- [5] M. Rouse, et J.P. Sullivan, « Mise en œuvre du Zero Trust dans des environnements de cloud hybride : défis et stratégies », Journal of Cybersecurity and Privacy, vol. 1, no 4, pp. 567-583, 2021.
- [6] D. Bhatt, « Sécuriser le périmètre : mise en œuvre de la sécurité Zero Trust face aux menaces mondiales », IEEE Communications Magazine, vol. 57, no 9, pp. 60-66, 2019.
- [7] E. Gilman, et B. Barth, Zero Trust
- [7] E. Gilman, and B. Barth, Zero Trust Security: How to Build Effective Defense Systems Against Today's Threats, O'Reilly Media, Inc., 2020.
- [8] N. Muldrow, "A Comprehensive Approach to Zero Trust Security," Journal of Network and Computer Applications, vol. 143, pp. 1-10, 2019.
- [9] J. Fruhlinger, "Zero Trust Security: An IT Leader's Guide," CSO Online, 2018.
- [10] R.D. Smith, "Microsegmentation Strategies for Zero Trust Implementations in Hybrid Clouds," IEEE Cloud Computing, vol. 6, no. 2, pp. 44-52, 2019.
- [11] S. Pearson, and G. Watson, "An Architecture for Privacy-Enhanced Cloud Computing," IEEE Security & Privacy, vol. 17, no. 2, pp. 30-39, 2019.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You for your attention

