

Review of the introduction of a thesis in Cybersecurity

Prepared by

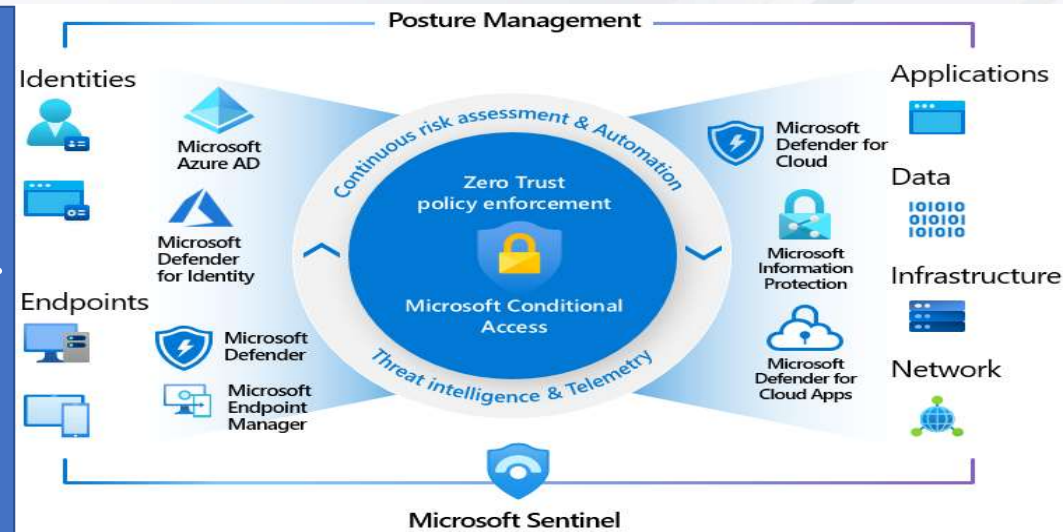
ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 2

I have chosen a thesis titled: "Analysis and Design of a Zero Trust-Based Cybersecurity Framework for the Protection of Hybrid Cloud Infrastructures." This research explores how the Zero Trust Security model can enhance the security of hybrid Cloud environments, where resources are distributed between on-premises servers and the public Cloud.



Introduction

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

As part of the "Critical Studies 2" module, I am presenting today the second task, which involves critiquing the introduction of a thesis in my field.

Definition of the subject and the 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.

1. Introduction

The rise of cloud computing has transformed how organizations handle data and applications, ushering in a new era of hybrid cloud setups that blend public cloud, private cloud, and on-premises resources. These environments promise flexibility, scalability, and cost-effectiveness but also introduce complex security challenges beyond the capabilities of traditional perimeter-based models [1]. Enter the Zero Trust architecture, founded on the principle of "never trust, always verify," which has emerged as a holistic solution for safeguarding modern digital ecosystems [2].

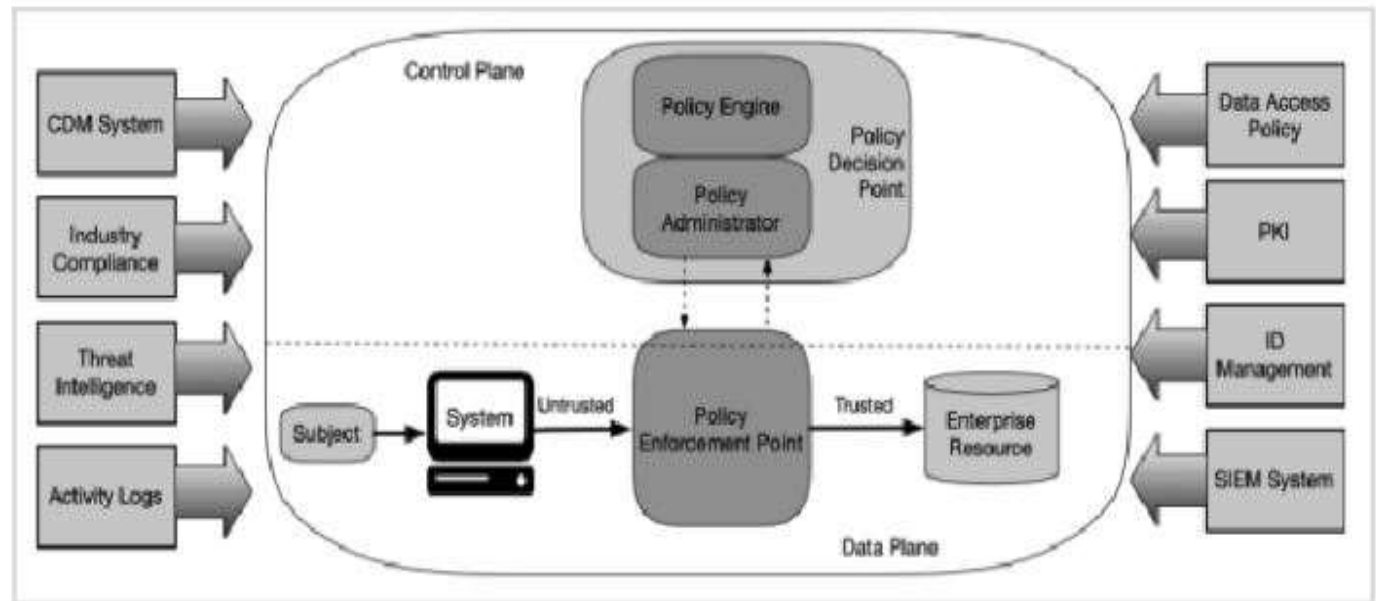
Zero Trust upends conventional security thinking by discarding the notion of inherent Trust for any entity, whether internal or external, to the network perimeter. Instead, it mandates continual verification of all users and devices, regardless of their location, before granting resource access [3]. This paradigm shift holds particular relevance in hybrid cloud scenarios, where resource dynamics and blurred perimeters demand a more nuanced and adaptable security stance [4]. Implementing Zero Trust in hybrid cloud environments presents both challenges and opportunities. While it provides a robust framework for safeguarding sensitive assets across diverse infrastructures, its adoption requires meticulous planning, strategic investments, and surmounting technical and organizational barriers [5].

References and research sources

In the second section of the introduction, the researcher cites several reliable sources, including:

- ❑ **NIST SP 800-207 (Zero Trust Architecture),**
- ❑ **Gartner reports (2022),**
- ❑ **and some recent articles on hybrid cloud security.**

✓ This shows that the introduction is not devoid of credible scientific references. However, some references are poorly integrated: the researcher mentions the authors' names without always citing the years or explaining the links between previous work and their topic. A good introduction should contextualize these references to show how they lead to the current problem.



NIST SP 800-207 Zero Trust Architecture

Justification of the choice of topic and importance of the study

We observe the section where the researcher justifies the choice of the topic. He **highlights the increase in cyberattacks targeting hybrid Cloud** environments and the ineffectiveness of traditional approaches based on internal trust.

- ✓ The **justification** is relevant and well-argued.
- ✓ The author emphasizes the importance of the **Zero Trust model**, which is based on the principle 'Never Trust, Always Verify.' However, he could have gone further by citing **real attack cases** or **quantitative studies** to support the severity of the problem. Thus, the justification is good, but it **lacks concrete data that would have strengthened** scientific credibility.

Explicit reference to the study's problem

The introduction contains an implicit reference to the problem, but **the researcher does not clearly formulate it** in the form of a question or hypothesis.

A sentence such as:

"The absence of a standardized Zero Trust framework for hybrid architectures limits the resilience of companies against persistent threats."

would have helped **to better anchor the issue**.

In scientific research, **clarity of the problem** is essential to guide the methodology and objectives. Here, this clarity is partially lacking.

Study population and limitations

The introduction **briefly mentions the scope of the study**, namely hybrid Cloud infrastructures in medium-sized companies. However, **it does not explicitly indicate the population studied**, nor the limitations of the work (for example: technological scope, types of Cloud analyzed, tools used).

This would have been **useful to clearly define the field of application** and avoid undue generalizations.

Study variables

The researcher mentions several **technical parameters** — such as the detection rate, latency time, and confidence level — but without defining them as **research variables**. It would have been preferable to specify:

- ❑ **the dependent variable:** the security level measured by the detection rate,
- ❑ **and the independent variables:** access policies, network segmentation, or Zero Trust protocols. Controlling these variables is essential to give the study an **experimental and scientific dimension**.

Overview and importance of the study

Finally, the last part of the introduction provides **an overview of the thesis structure** and highlights the importance of the work for companies adopting hybrid Cloud models.

✓ This is good practice, as it helps the reader anticipate the flow of the research. However, the introductory conclusion would have benefited from summarizing **the main objectives** in clear bullet points, in order to outline the rest of the thesis.

CONCLUSION

In summary, the introduction of this thesis on the **Zero Trust framework for hybrid Cloud is well-structured**, rich in references, and demonstrates a good understanding of the current context. The areas for **improvement concern the explicit formulation of the problem**, the definition of variables, and the delineation of the population and study boundaries. This critique allowed me to deepen my ability to analyze **scientific introductions in cybersecurity**, by identifying the criteria of rigor and clarity required at the doctoral level.
Thank you for your attention.

- [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

