

Task 5 – Review of Previous Studies

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

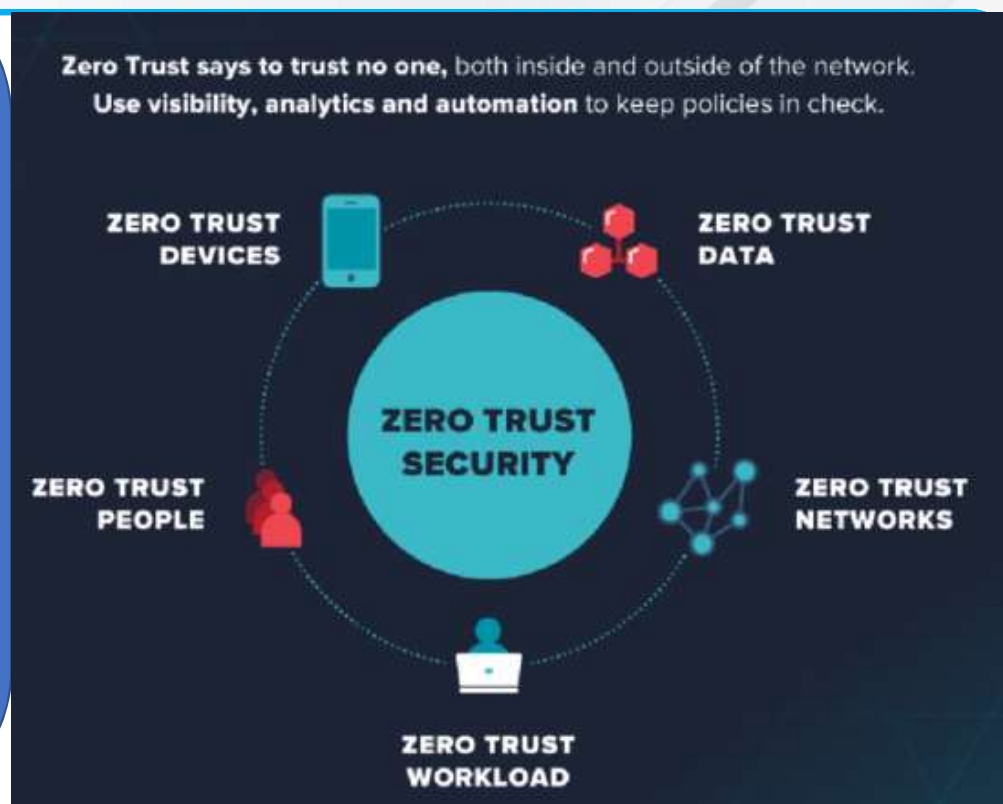
Task 5

INTRODUCTION

Hello everyone,
I am Ali Mmadi, a PhD student in Information Technology, specializing in Cybersecurity. In this fifth task of the Critical Studies 2 module, I will analyze the review of previous studies in the thesis entitled:

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

This critique aims to evaluate the quality, diversity, and relevance of the previous studies used in this thesis, while identifying the strengths, weaknesses, and gaps in this literature review.



Coverage and updates of previous studies

The researcher relies on about twenty academic references, most of which date from 2018 to 2023, demonstrating an effort to stay current. Among the cited sources, recent works include:

NIST SP 800-207 (2020) on the Zero Trust model,

AlHogail & Mirza (2023) on implementation challenges in the Cloud,

Zhang & Chen (2021) on adaptive access control

Coverage and Recency of Previous Studies



The researcher references a range of recent studies



However, few studies before 2015 are discussed

✓ Critical analysis:

These references are relevant and reflect recent developments in the field.

⚠ However, the review includes almost no studies before 2015, whereas precursor models like BeyondCorp (Google, 2014) could have provided historical context for the Zero Trust concept.

Thus, the temporal coverage is good but unbalanced: it favors recent publications at the expense of theoretical foundations.

Diversity and types of sources

The researcher mainly relies on indexed **scientific articles** (IEEE, Elsevier, **Springer**), which demonstrates a rigorous approach.

However, he cites very **few industry reports** or **specialized books**, which are essential for understanding the practical challenges of cybersecurity in businesses.

✓ Positive points:

Good use of validated academic sources.

⚠ Points to improve:

Limited diversity in the types of documents used.

Lack of **professional reports** (such as those from Gartner or Microsoft Security) which would have enriched the practical perspective on the subject.

In doctoral research, it is essential to **combine academic** and **industry sources** to balance theory and application.

Balance between old and recent studies

The literature review places a strong emphasis on the 2018–2023 period, reflecting the rapid developments in Cloud and Zero Trust.

However, no references prior to 2010 are discussed, particularly those related to perimeter security or the evolution of access models.

⚠ This creates a historical imbalance.
A balanced review should include:

recent studies for technical developments,
and older studies for context and conceptual foundations.

Thus, the review appears technically rich but theoretically incomplete.

**Balance between older
and recent studies**



**Balance between older
and recent studies**

Balance between old and recent studies

The majority of the cited studies are presented in a **descriptive manner**: the author summarizes the results **but does not analyze the limitations** of previous approaches.

✓ **Strengths:**

The studies are correctly cited and integrated throughout the text.

⚠ **Weaknesses:**

Little analysis of the **methodologies used** (for example, distinction between experimental and conceptual studies).

Lack of **critical comparison**: the researcher could have contrasted the approaches of **NIST, Gartner, and Google BeyondCorp** to highlight differences in the implementation of Zero Trust.

A constructive critique would have highlighted points of convergence and contradiction, strengthening the justification for the new study.

Identifying gaps in research

The thesis identifies a main gap:

“Few studies have examined Zero Trust implementation in hybrid Cloud environments with empirical validation.”

✓ This is a relevant and well-**formulated observation**, as most previous research remains **theoretical**. However, the researcher could have specified:

- **The level of missing empirical validation,**
- **The unexplored methods (for example, comparative quantitative studies).**

As a critic, I consider the **gap to be correct but incomplete**: it does not show enough how this study **concretely addresses** this shortcoming.

CONCLUSION

In conclusion:

- ☐ The review of previous studies is **recent** and **relevant**,
- ☐ but it lacks **diversity in sources**,
- ☐ and **an in-depth critical analysis** of the methodologies.

For a doctoral work, such a review should aim to **connect previous studies**, **discuss their limitations**, and explicitly **justify the scientific contribution**.

Thank you for your attention.

I am **Ali Mmadi**, a PhD student in Cybersecurity, and this was my **Task 5 – Critique of Previous Studies**.

Zero Trust & Cloud Security

1) Zero Trust & Cloud Security

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).

Zero Trust Architecture (NIST Special Publication 800-207).

National Institute of Standards and Technology.

2) AlHogail, A., & Mirza, A. (2023).

Challenges and Opportunities of Implementing Zero Trust Architecture in Cloud Computing.

IEEE Access, 11, 15523–15540.

3) 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.

4) Zhang, X., & Chen, L. (2021).

Adaptive Access Control for Hybrid Cloud Security using Zero Trust Principles.

Journal of Cloud Computing, 10(12), 1–15.

5) Microsoft Security (2023).

Zero Trust Adoption Strategy for Hybrid Enterprises.

Microsoft Whitepaper.

Cybersecurity Models & Frameworks

6) Gartner (2023).

Hybrid Cloud Security: Strategic Roadmap for Implementing Zero Trust.

7) Kindervag, J. (2010).

No More Chewy Centers: Introducing Zero Trust.

Forrester Research Report.

(Foundational reference establishing the Zero Trust model)

Intrusion Detection & Anomaly Detection

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) Shin, D., & Park, S. (2022).

Modeling the Impact of Zero Trust Policy Enforcement on Cloud Security Performance.

Computers & Security, 113, 102553.

Hybrid Cloud Architecture

10) Marinos, A., & Briscoe, G. (2009).

Community Cloud Computing.

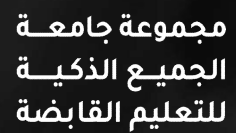
IEEE Cloud Computing Conference.

(Foundational reference for hybrid and community Cloud concepts)

11) Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013).

An Analysis of Security Issues for Cloud Computing.

Journal of Internet Services and Applications, 4(1), 5.



MIDOCEAN
UNIVERSITY



Thank you!!!!!!!!!!!!!!!!!!!!

