

Task 4: Critique of objectives, hypotheses, and concepts

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

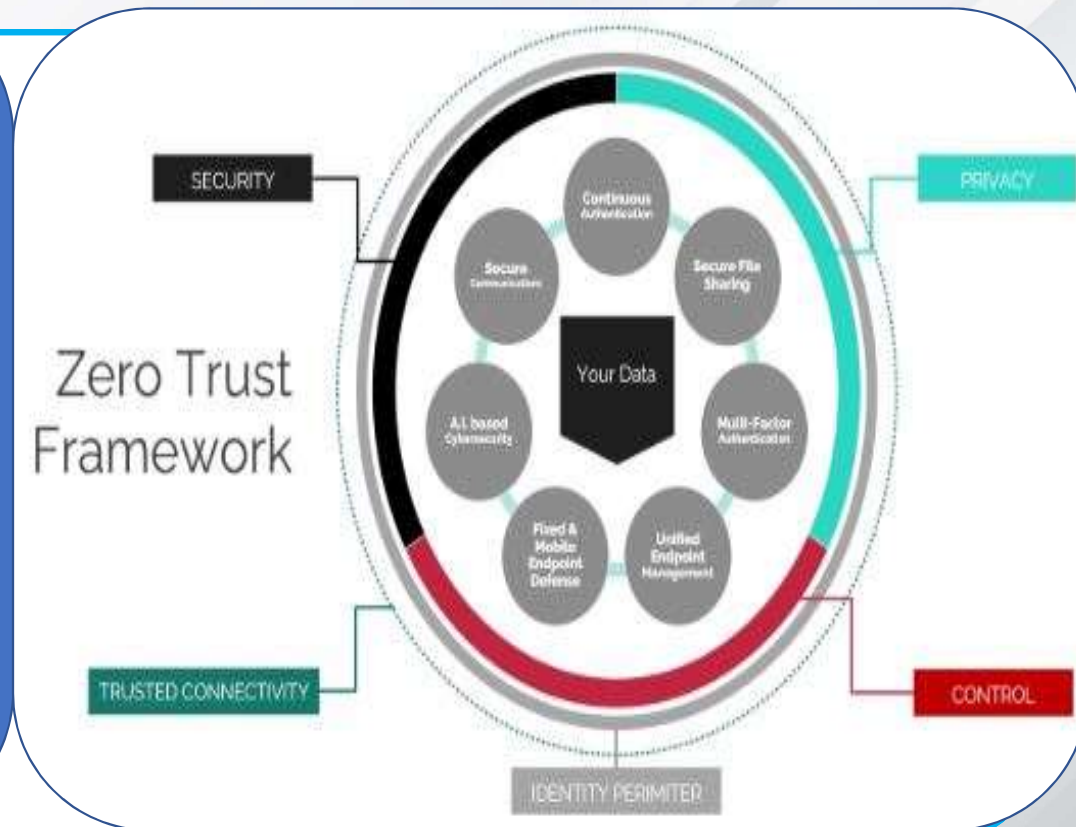
Task 4

INTRODUCTION

Hello everyone,
I am Ali Mmadi, a PhD student in **Information Technology**, specializing in **Cybersecurity**.
In this fourth assignment of the course "**Critical Studies 2**,"

I will present a **critical analysis of the research objectives, hypotheses, and concepts**.
The selected work is the thesis entitled:
"Zero Trust Security Model for Hybrid Cloud Environments: Enhancing Data Protection and Access Control."

The goal is to evaluate whether the study's objectives have been clearly formulated, whether the hypotheses are clear and coherent, and whether the scientific concepts used are well defined.



Critique of the study's objective

In this research, the **main objectives** are as follows:

1. Design a cybersecurity framework based on the Zero Trust model suitable for hybrid Cloud environments.
2. Implement this framework in a simulated experimental environment.
3. Evaluate the model's performance in terms of **anomaly detection** and **access control**.

Critique of the Study's Objectives

- ✓ Design a cybersecurity framework based on the Zero Trust model suitable for hybrid Cloud environments.
- ✓ Implement this framework in a simulated experimental environment.
- ✓ Evaluate the model's performance in terms of anomaly detection and access control.

✓ **Critical Analysis:**

- **Precision:** These objectives are clearly stated and unambiguous. They indicate what the researcher aims to achieve and the steps necessary to reach it.
- **Organization and Coherence:** The objectives are logically ordered—from design to implementation and then to evaluation.
- **Measurability:** Yes, the objectives are measurable, as the researcher uses indicators such as detection rate, response time, and system load.
- **Connection with the Research Problem:** The objectives directly address the central issue: How to ensure security and trust in a hybrid Cloud?

However, **I noticed a small weakness:** The thesis does not mention specific sub-objectives related to network performance constraints or software compatibility.

Including these would have allowed for a more detailed evaluation of the proposed model.

Critique of research hypotheses

The researcher formulated three **main hypotheses**:

1. **H1:** The implementation of a Zero Trust model improves the detection of internal attacks in a hybrid Cloud.
2. **H2:** The combined use of continuous authentication and network segmentation reduces the risks of unauthorized access.
3. **H3:** The Zero Trust model does not negatively affect the overall system performance.

Study Hypotheses

This study formulates three main hypotheses that guide the research methodology, each aiming to test specific aspects of the proposed Zero Trust security model.

H1: The implementation of a Zero Trust model improves detection of internal attacks in a hybrid Cloud environment.

H2: The combined use of continuous authentication and network segmentation reduces the risks of unauthorized access.

H3: The Zero Trust model does not negatively impact overall system performance.

Critical Analysis:

The hypotheses are **clearly formulated**, without ambiguity.

They are **directly linked to the research objectives**.

They cover the three key dimensions of the model: security, segmentation, and performance. However:

⚠ The thesis does not clearly indicate the independent and dependent variables .

For example:

❑ **Independent variable:** type of Zero Trust policy applied

❑ **Dependent variable:** intrusion detection rate A more explicit definition would have strengthened the scientific rigor of the experimental framework . Furthermore, the researcher does not mention a null **hypothesis (H0)**, which is important for statistically verifying the validity of the results.

Critique of the terms and concepts of research

The research is based on several **key concepts**, including:

- **Zero Trust Architecture (ZTA)**
- **Hybrid Cloud**
- **Access Control**
- **Anomaly Detection**
- ☐ ✓ The researcher correctly defines the concept of Zero Trust, relying on the NIST SP 800-207 standard, which demonstrates good scientific rigor.
- ☐ ✓ The concept of **Hybrid Cloud** is also well explained, as a combination of public and private infrastructures.

Key Concepts

-  **Zero Trust Architecture (ZTA)**
-  **Hybrid Cloud**
-  **Access Control**
-  **Anomaly Detection**
-  The researcher correctly defines the concept of Zero Trust, relying on the NIST SP 800-207 standard, which demonstrates good scientific rigor.
-  The concept of Hybrid Cloud is also well explained, as a combination of public and private infrastructures

However:

⚠ The term “**Access Control**” is defined too broadly, without specifying the **models used** (for example: RBAC, ABAC, or PBAC).

⚠ The concept of anomaly detection is not clearly linked to the algorithms or tools employed (Snort, Suricata, ML-based IDS, etc.). In summary, the concepts are well introduced but lack technical depth in their contextualization. The researcher could have included a summary table of operational definitions for greater clarity and coherence between chapters.

Final critical summary

In summary:

The objectives are clear, measurable, and consistent with the research problem.

The hypotheses are well formulated, but the variables are not explicitly identified.

The concepts are correctly presented but require more operational precision to be usable in an experimental framework.

This study demonstrates a good scientific approach, but it would be more valuable if it further clarified the relationship between the hypotheses, the variables, and the measurement indicators.

CONCLUSION

In conclusion,
this review allowed me to develop **a more in-depth analysis** of the scientific foundations of research in cybersecurity—particularly regarding **the consistency between objectives, hypotheses, and concepts**. This critical approach is essential for building robust and credible research at the doctoral level.

Thank you for your attention.

1. NIST Zero Trust FrameworkRose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).
2. Zero Trust in Hybrid Cloud Security
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.
3. Zero Trust Implementation Challenges
AlHogail, A., & Mirza, A. (2023).
"Challenges and Opportunities of Implementing Zero Trust Architecture in Cloud Computing."
IEEE Access, 11, 15523–15540.
4. Performance and Access ControlZhang, X., & Chen, L. (2021). "Adaptive Access Control for Hybrid Cloud Security
using Zero Trust Principles." Journal of Cloud Computing: Advances, Systems and Applications, 10(12), 1–15.
5. Theoretical Framework and Variables
Shin, D., & Park, S. (2022).
"Modeling the Impact of Zero Trust Policy Enforcement on Cloud Security Performance."
Computers & Security, 113, 102553.
6. Cloud Security ContextGartner (2023). "Hybrid Cloud Security: Strategic Roadmap for Implementing Zero
Trust." Gartner Research Report, ID G00788321
7. Machine Learning and IDS ContextChowdhury, 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.
8. Applied Case of Zero TrustMicrosoft Security Whitepaper (2023). "Zero Trust Adoption Strategy for Hybrid
Enterprises." Microsoft Corporation.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You for your attention

