

**Presentation of the hypotheses,
objectives, and study variables
in cybersecurity research**

Prepared by

ALI MMADI, PhD student - Midocean University





Research Skills (1)

Task 6

ALI MMADI

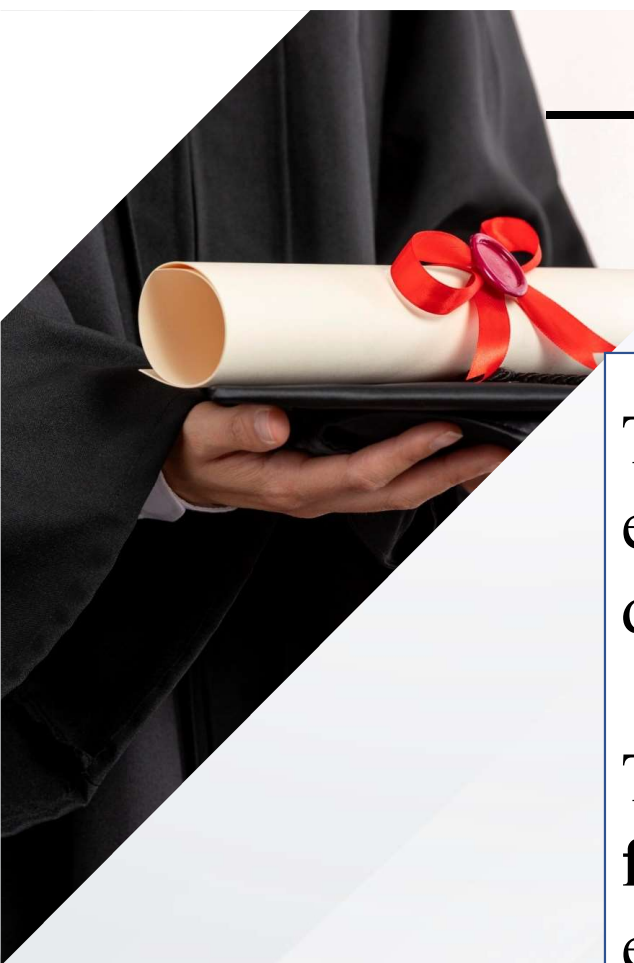
PhD student - Midocean University

www.midocean.ae

Selected scientific research: "Improving the security of critical networks in companies through advanced hashing functions"

INTRODUCTION

In this video 6, I will present to you a scientific research in the field of cybersecurity, and more specifically on securing critical networks in businesses using cryptographic hash functions. We will explore together the objectives of this research, the formulated hypotheses, as well as the study variables, clearly distinguishing between the independent variable and the dependent variable.



Research context

Today, critical business networks are particularly exposed to cyberattacks, including intrusions, data tampering, and Man-in-the-Middle attacks.

This study examined the use of **secure hashing functions** — such as SHA-256 or SHA-3 — to enhance the integrity of network communications and detect any unauthorized modifications to the data.

Research objectives

The research pursued the following objectives:

- 1) To evaluate the effectiveness of hash functions in protecting data packets circulating in a critical network.
- 2) To analyze the performance of these mechanisms in terms of speed and system load.
- 3) To determine whether hash functions allow for the automatic detection of alterations or data manipulations in network flows.

The main objective was therefore to verify whether hash functions can constitute a reliable solution for ensuring the integrity and security of critical communications.

Research hypotheses

Based on these objectives, several scientific hypotheses have been formulated:

Hypothesis 1: The use of hash functions significantly enhances the integrity of network packets in critical infrastructures.

Hypothesis 2: The performance of modern hash functions does not introduce excessive overhead on the network.

Hypothesis 3: There is a direct correlation between the type of hash function used and the rate of detection of data tampering.

Identification of variables

Among these hypotheses, let's take the first one as an example: "The use of hash functions significantly strengthens the integrity of network packets."

The independent variable here is: the use or non-use of a cryptographic hash function.

The dependent variable is: the level of data integrity transmitted over the network (measured by the rate of alteration or detected attack).

It is thus the use of hashing that acts as the triggering factor, and data integrity is the observed result.

CONCLUSION

In summary, this study shows how a rigorous scientific approach based on clear objectives, logically formulated hypotheses, and a good understanding of the variables allows us to address critical issues in cybersecurity.

The identification of variables is essential for designing reliable experiments and validating the proposed hypotheses.

Thank you for your attention.

List of references

- 1) Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson Education. A reference work that covers hash functions, their role in network security, and measurable variables in cryptography.
- 2) Wang, X., & Yu, H. (2005). How to Break MD5 and Other Hash Functions. In Advances in Cryptology – EUROCRYPT 2005, Springer, pp. 19–35. A technical study demonstrating the vulnerabilities of certain hash functions, useful for understanding the security issues in critical networks.
- 3) Alsmirat, M. A., Jararweh, Y., Al-Ayyoub, M., & Gupta, B. (2017). Internet of Things: Security and Privacy. In Handbook of Computer Networks and Cyber Security, Springer. Includes an analysis of the use of hash functions in securing sensitive network communications.

- 4) Bellare, M., & Rogaway, P. (2005). Introduction to Modern Cryptography. Lecture notes. Educational document on the mathematical and functional foundations of cryptographic hashes.
- 5) Kaur, G., & Singh, M. (2016). A Review on Secure Hash Functions in Cryptography. International Journal of Computer Applications, 144(6), 5–9.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

