

**Importance, objectives, and hypotheses
of scientific research in cybersecurity**

Prepared by

ALI MMADI, PhD student - Midocean University



Research Skills 1

Task 5

ALI MMADI

PhD student - Midocean University

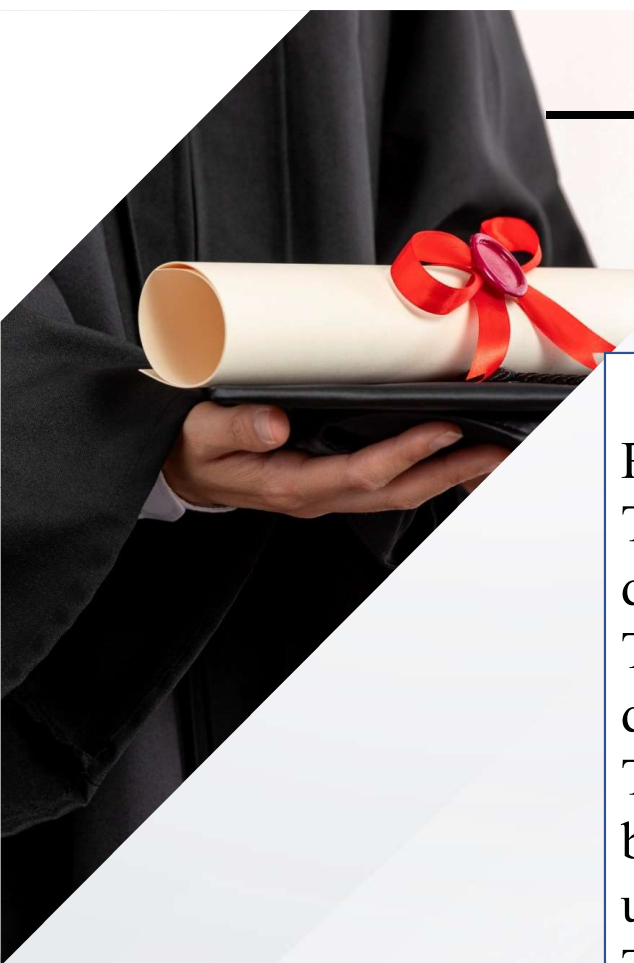
www.midocean.ae

Selected scientific research: “ Proactive Detection of Ransomware Attacks Using Deep Learning ”

I will present an important scientific research in the field of cybersecurity.

It focuses on the proactive detection of ransomware attacks using artificial intelligence, and more specifically deep learning.

We will discuss together the importance of this research, its main objectives, as well as the scientific hypotheses that guided the researchers throughout their study.



Importance of research

Ransomware attacks are today one of the biggest cyber threats. They involve encrypting the files of a user or a company, then demanding a ransom in exchange for the decryption key.

The problem is that most antivirus software or security systems detect the attack after it has started, sometimes too late.

That is why this study is essential: it seeks to predict these attacks before they cause damage, by analyzing suspicious behaviors using deep learning.

This research is therefore crucial to protect sensitive data, prevent economic losses, and strengthen the security of critical systems, such as those of hospitals or governments.

Research objectives

Researchers have set several clear objectives for this study:

- 1) First, to design a system capable of detecting ransomware before encryption by observing weak signals in systems.
- 2) Next, to analyze the typical behaviors of ransomware in the early moments of their execution.
- 3) To compare different deep learning algorithms, such as LSTM neural networks or CNN convolutional networks.
- 4) And finally, to integrate this system into a real network environment to see if it is applicable on a large scale, such as in businesses.

These objectives allow us to go beyond theory and propose a solution usable under real conditions.

Research hypotheses

To guide this study, the researchers formulated several scientific hypotheses.

The first hypothesis is that:

✓ It is possible to detect ransomware before encryption, simply by observing its abnormal behaviors, such as unusual file access or suspicious network connections.

Second hypothesis:

✓ Deep learning models, such as recurrent neural networks, are more effective than traditional methods for recognizing these behaviors in real-time. And finally, the third hypothesis:

✓ Once trained, these models can be integrated into current cybersecurity tools to strengthen defenses without compromising system

CONCLUSION

this research is an excellent example of how the scientific method can be applied to concrete and urgent problems. By analyzing the importance of the subject, defining measurable objectives, and formulating strong hypotheses, the researchers have paved the way for innovative solutions to prevent ransomware attacks. Thank you for your attention, and see you soon for the next video.

List of references

- 1) Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). *Detecting ransomware using deep learning models*. Procedia Computer Science, 165, 631–639.
- 2) Alazab, M., Awajan, A., Mesleh, A., et al. (2021). *COVID-19 and ransomware: A systematic review*. Computers & Security, 110, 102384.
- 3) Rigaki, M., & Garcia, S. (2018). *Bringing a GAN to a knife-fight: Adapting malware communication to avoid detection*. IEEE Security & Privacy Workshops.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

