

Presentation of two previous studies in cybersecurity

Prepared by

ALI MMADI, PhD student - Midocean University



Research Skills (1)

Task 8

ALI MMADI

PhD student - Midocean University

www.midocean.ae

INTRODUCTION

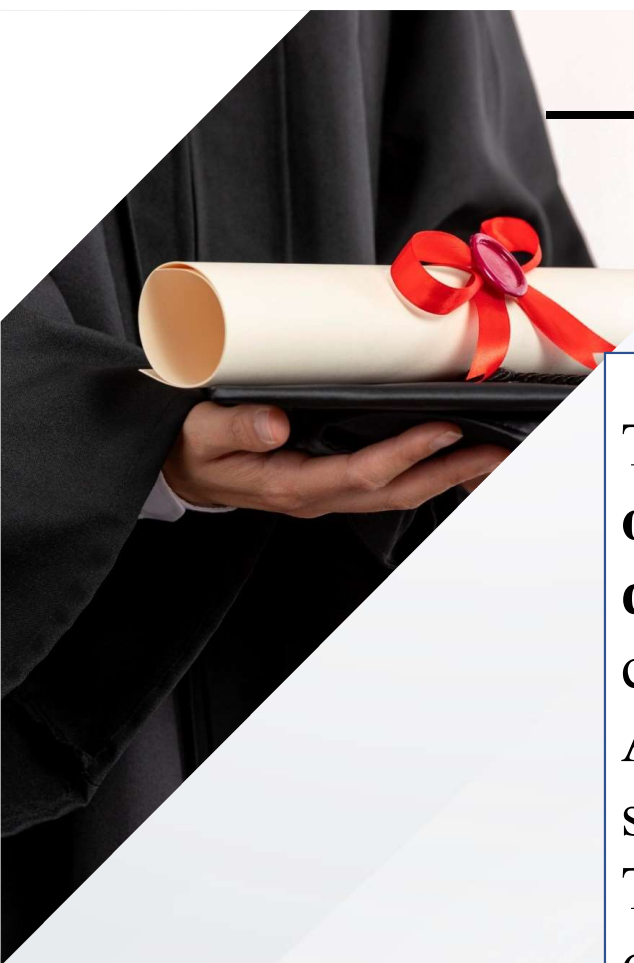
Today, as part of our study on previous research, I am going to present to you two scientific studies in the field of cybersecurity. We will look together at their **context, objectives, the methods used, the main results, and above all**, the importance of these studies for future research.

This presentation illustrates the correct way to cite and utilize previous works in a scientific project.

Importance of previous studies Previous studies play a crucial role in any scientific research. They allow for:

- 1) avoiding the repetition of work that has already been done,
- 2) building on existing results to delve further,
- 3) and correctly guiding new hypotheses and methods.

Now let's move on to the first study.



First study: Context and reference

The first study is titled: "**Automated dynamic analysis of ransomware: Benefits, limitations and use for detection**," published in 2016 by Sgandurra and his colleagues.

At the time, **ransomware** was becoming one of the most serious threats to businesses and critical infrastructures. These malicious programs encrypt victims' data and demand a ransom to restore it.

Traditional security solutions struggled to detect these attacks in time.

Objective of the study

The objective of this research was **to develop an automated** detection system capable of identifying ransomware before it encrypts the files on a computer.

The main idea was **to dynamically analyze the behavior** of suspicious programs, rather than relying solely on known signatures.

Method and results

Researchers executed several samples of ransomware in a virtual environment and observed their actions in real time. They then applied **machine learning** algorithms to recognize characteristic behaviors.

The results showed a **detection rate exceeding 95%**, demonstrating the effectiveness of the dynamic approach. This study is now widely cited for the development of intelligent antivirus solutions.

Second study :Context and reference

The second study is titled: "**Anomaly detection in a cyber physical system using relevance vector machine**," conducted by Adepu and Mathur in 2016.

It focuses on **the security of industrial networks**, also known as SCADA systems, used in critical infrastructures such as power plants and factories.

These systems have become a primary target for cyberattacks, posing a major risk to national security.

Objective of the study

The objective of this research was to detect anomalies in industrial systems in order to prevent sabotage and intrusions.

The researchers used a machine learning-based approach called Relevance Vector Machine. This technique allows for the automatic classification of normal and suspicious behaviors in an industrial network.

Method and results

Researchers simulated a SCADA network, collected sensor and command data, and then trained their learning model. The results are very encouraging: the algorithm achieved an **anomaly detection accuracy of over 97%**, helping to strengthen the resilience of critical infrastructures.

This study has paved the way for many other research efforts on protecting industrial systems against cyberattacks.

Link with scientific research

Discussion and importance

These two previous studies are **an excellent example of complementarity**:

- ❖ **The first focuses on protecting workstations against ransomware.**
- ❖ **The second targets industrial network security.**

Together, they provide knowledge and concrete results that new research can leverage to create more comprehensive and robust cybersecurity solutions.

CONCLUSION

In conclusion, this presentation showed how to properly integrate previous studies into scientific research.

We have seen:

- The context
- The objectives
- The methods
- And the results of the two selected studies.

Previous studies are essential for building solid research, avoiding redundancies, and progressing more quickly in the fight against cyber threats.

Main research references

- 1) Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. (2016). *Automated dynamic analysis of ransomware: Benefits, limitations and use for detection*. arXiv preprint arXiv:1609.03020.
- 2) Adep, S., & Mathur, A. (2016). *Anomaly detection in a cyber physical system using relevance vector machine*. In *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)* (pp. 130–137). IEEE.

↪ Lien vers IEEE Xplore



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

