

**Presentation of a study using
the experimental method
applied to cybersecurity**

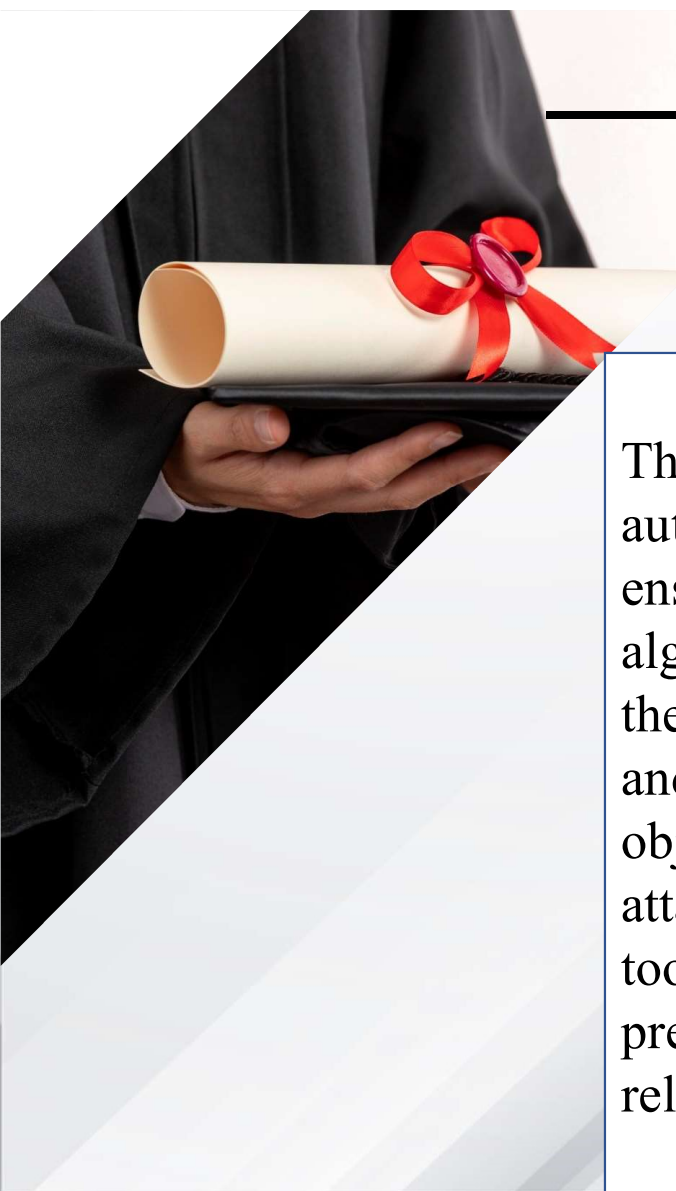
Prepared by

ALI MMADI, PhD student - Midocean University



INTRODUCTION

Hello everyone, In this video, I will present to you a scientific study conducted in the field of cybersecurity. This study focuses on a very current topic: the detection of intrusions in computer networks, meaning the detection of cyber attacks such as hacking attempts or unauthorized intrusions. To conduct this study, the researchers used the experimental method, a rigorous approach that allows for testing a hypothesis through controlled experiments. Let's look together at what the objectives of this research were and how it was conducted.



Research objectives

The study had several objectives: First, to effectively and automatically detect intrusions in a network, which is essential to ensure data security. Next, to compare several machine learning algorithms, such as Random Forest or SVM, to determine which is the most effective. And finally, to propose a solution that is faster and more reliable than traditional detection methods. These objectives are very important, as in the field of cybersecurity, attacks are becoming increasingly sophisticated, and traditional tools are no longer sufficient. Therefore, this study allows for the prediction and control of large-scale incidents, highlighting the relevance of scientific research in this field.

Scientific method used

Researchers followed the experimental method, which consists of several stages: First, they observed the problem: attacks are frequent and detection tools are not effective enough. Next, they formulated a hypothesis: some machine learning algorithms might detect intrusions better than others. Then, they set up an experimentation: They selected databases like KDD Cup 99 or NSL-KDD, which contain records of network traffic with known attacks. Then, they applied several machine learning algorithms to these data: SVM, Random Forest, KNN, etc. Finally, they measured the performance: detection accuracy, false positive rate, and execution speed. After that, they compared the results and determined which algorithm was the most effective. This is a rigorous, reproducible approach based on concrete data, which aligns exactly with the spirit of the experimental method.

Results and importance

The results of the study showed that certain algorithms, such as Random Forest, achieved better results in terms of accuracy and speed. This means that computer security can be improved by using smart and automated tools. This research therefore has a direct impact: it can be used to strengthen the security of companies, administrations, or even critical systems such as hospitals or banks.

CONCLUSION

In conclusion, this study shows that the experimental method allows for testing concrete solutions to a real problem. Thanks to a rigorous scientific approach, the researchers were able to propose an innovative and applicable solution in the real world. This is a great example of how scientific research can address current challenges in cybersecurity.

List of references

- 1) Moustafa, N., & Slay, J. (2016). *The UNSW-NB15 dataset for network intrusion detection systems (NIDS)*. 2015 Military Communications and Information Systems Conference (MilCIS), IEEE.
- 2) Ahmed, M., Mahmood, A. N., & Hu, J. (2016). *A survey of network anomaly detection techniques*. Journal of Network and Computer Applications, 60, 19-31.
- 3) Lippmann, R. P., et al. (2000). *The 1999 DARPA off-line intrusion detection evaluation*. Computer Networks, 34(4), 579–595.
- 4) Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). *A detailed analysis of the KDD CUP 99 data set*. IEEE Symposium on Computational Intelligence for Security and Defense Applications.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

