

Comparative analysis of
methods for presenting previous
studies in scientific research
applied to cybersecurity.

Prepared by

ALI MMADI, PhD student - Midocean University



Research Skills (2)

Task 3

ALI MMADI

PhD student - Midocean University

www.midocean.ae

1. Introduction

Hello everyone, My name is **Ali Mmadi**, a PhD student in **Information Technology**, specializing in Cybersecurity.

In this third task of the Research Skills 2 course, I will present **two scientific methods** used to **formulate and present previous studies** in a research paper.

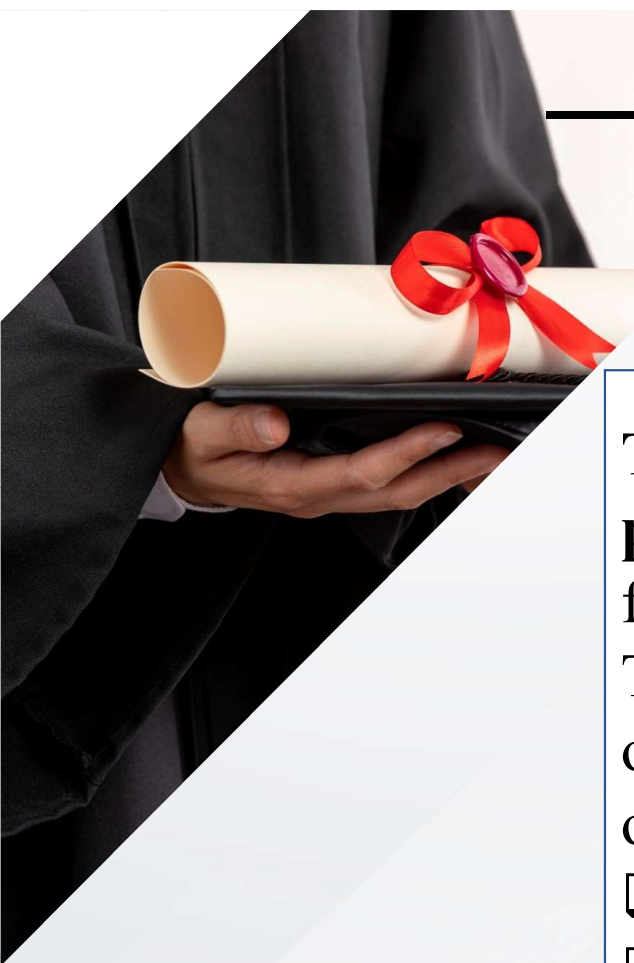
These two methods are:

1. **The chronological method,**
2. **The thematic or subject-based method.**

I will illustrate each method with concrete examples from the field of **cybersecurity of Cloud infrastructures and intrusion detection systems.**



Thematic
vs
Chronological



2. First method: the chronological ranking method

The chronological classification method involves presenting previous studies in order of time, that is, from the oldest to the most recent.

This approach allows for showing the scientific evolution of the subject by explaining how research has progressed over the years. In this method, the researcher:

- ☐ **First presents the foundational works,**
- ☐ **Then the intermediate research,**
- ☐ **And finally the most recent studies, highlighting the advances and limitations of each period.**

Example in the field of cybersecurity:

- In 2004, the first research on intrusion detection was based on static signatures (Snort, Bro).
- By 2015, researchers such as Sommer and Paxson proposed behavioral approaches using network statistics.
- And from 2018 onwards, studies incorporated artificial intelligence and machine learning to automatically analyze threats in Cloud environments.

This chronological presentation shows **the evolution of cybersecurity**: from reactive rule-based detection → to proactive AI-based detection.

Advantage: it highlights scientific progress.

Limitation: it remains descriptive and does not compare the approaches.

3.Second method: the thematic method

The thematic method, also called the subject-based method, involves grouping previous studies according to themes or sub-domains. This approach is very useful in cybersecurity, as it allows the literature to be structured according to the main axes of the studied problem. In this method, the researcher:

- Identifies the main themes related to the issue,
- Classifies studies according to these themes,
- And demonstrates how each group of research contributes to solving a part of the problem.

Studies can be organized into three main themes:

1. Signature-based intrusion detection models.

➤ **Example:** Work by Roesch (Snort, 1999), effective but limited against new threats.

2. Machine learning models.

➤ **Example:** Al-Qatf et al., 2018, using neural networks to classify attacks.

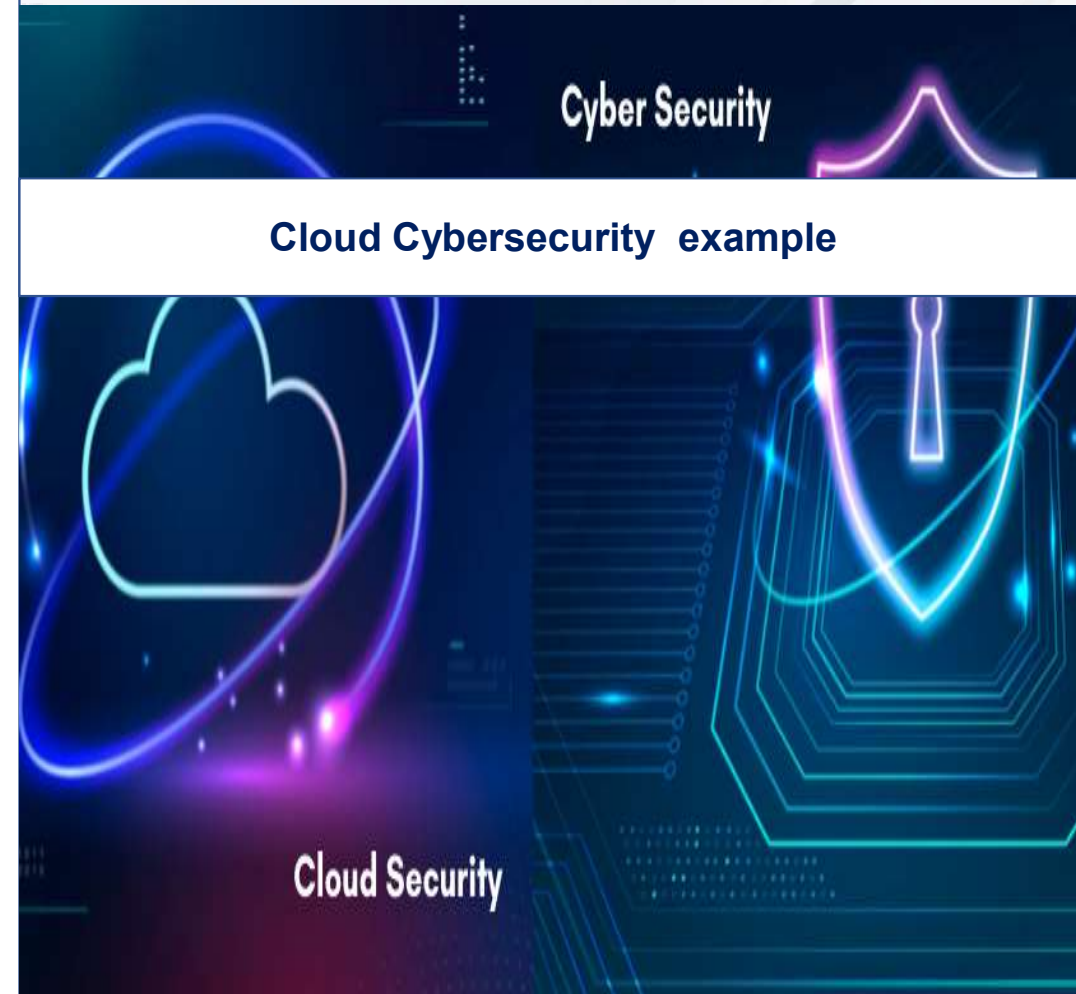
3. Hybrid and intelligent approaches.

➤ **Example:** He & Chan, 2022, combining deep learning and behavioral analysis in the Cloud.

This method provides a **comparative and structured view** of existing contributions.

Advantage: it promotes critical analysis and synthesis.

Limitation: it requires thorough reading and good intellectual organization.



4. Discussion and comparison of the two methods

When comparing the two methods:

- ❑ **The chronological method is useful for showing the historical evolution of a field.**
- ❑ **The thematic method is preferable when the field is rich and multidimensional, such as cybersecurity.**

In my research practice, I often use a combination of the two methods: I start with a brief chronological overview to show the development of the field, then I structure the studies by **thematic categories** to analyze recent contributions in depth

5. Conclusion

In summary:

- ❖ **Previous studies form the foundation of all scientific work.**
- ❖ **The chronological method shows progression over time,**
- ❖ **While the thematic method allows for an analytical and critical understanding of the field.**

These approaches are essential in the field of cybersecurity, where technology evolves rapidly and research must continually adapt. Thank you for your attention.

Bibliographic reference

1. ***Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach for Intrusion Detection in Cloud Environments. Future Generation Computer Systems, 89, 347–359.***
2. ***He, H., & Chan, S. (2022). Hybrid AI Models for Cloud Intrusion Detection: A Review. IEEE Access, 10, 20315–20329.***
3. ***Roesch, M. (1999). Snort – Lightweight Intrusion Detection for Networks. USENIX Conference.***
4. ***NIST SP 800-94 (2021). Guide to Intrusion Detection and Prevention Systems (IDPS). 
<https://csrc.nist.gov/publications/detail/sp/800-94/final>***



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

