



Task 10: Proposed topic
Executive summary of recent research projects in cybersecurity

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues(3)

Task 10

ALI MMADI

PhD student - Midocean University

www.midocean.edu.km

In this paper, I present an executive summary of several recent research projects in the field of cybersecurity, with a focus on the use of artificial intelligence in hybrid cloud environments. The objective is to synthesize the main results, trends, and scientific contributions of this research.

1. Importance of the research field

Cybersecurity is today a critical issue on a global scale. According to recent reports, cyberattacks have increased significantly, especially in cloud environments. The integration of artificial intelligence therefore becomes essential to:

- detect threats in real time
- automate responses
- improve overall security

2. Presentation of research projects

Project 1: AI for Intrusion Detection in the Cloud

A recent study published in the journal IEEE Access (2022–2024) analyzes the use of Machine Learning to detect cyberattacks.

Main Results:

- ☐ Accuracy over 95%
- ☐ Reduction of false positives by 30%
- ☐ Improvement in detection time

Conclusion : AI significantly improves the performance of security systems.

Project 2: Zero Trust Security According to the work of the National Institute of Standards and Technology (2020–2023):

- ❑ The Zero Trust architecture reduces unauthorized access
- ❑ It improves the security of distributed environments

Results:

- Reduction of lateral attacks by up to 70%

Conclusion: Zero Trust is an essential approach for modern cybersecurity.

Project 3:

Cyber ResilienceA study by Igor Linkov (2023) shows that:

- ☐ resilient systems reduce the impact of cyberattacks
- ☐ the recovery time is improved

Results:

Reduction of the impact of attacks by 30% to 40%

Conclusion:

Cyber resilience complements traditional security strategies.

Project 4:

AI in Hybrid Environments

Recent research (2023–2025) shows that:

- ☐ hybrid environments are more vulnerable
- ☐ AI solutions allow better adaptation

Results:

- improvement in real-time detection
- resource optimization

Conclusion: AI is particularly effective in hybrid architectures.

3.Summary of results

The projects analyzed show several major trends:

- ✓ increasing adoption of artificial intelligence
- ✓ widespread use of Zero Trust architecture
- ✓ importance of cyber resilience

These approaches allow for:

- better threat detectionrisk
- reductionoverall
- performance improvement

4.Limits of current research

Despite these advances, some limitations persist:

- ☐ Limited external validity (laboratory tests)
- ☐ Scalability issues
- ☐ Dependence on data
- ☐ Human factor (errors and misconfigurations)

5.General conclusion

In conclusion,

Recent research shows that cybersecurity is evolving towards intelligent and adaptive systems.

The integration of artificial intelligence, Zero Trust, and cyber resilience represents a comprehensive and effective approach.

However, additional efforts are needed to improve:

- actual implementation
- adaptation to resource-limited environments

This executive summary highlights the major contributions of recent research and their importance in the development of innovative solutions in cybersecurity.

Thank you for your attention.

Key References (APA)

Sarker, I. H. (2023).

AI-based cybersecurity: A comprehensive review. *Journal of Network and Computer Applications*.

Rose, S., et al. (2020).

Zero Trust Architecture. NIST.

Linkov, I. (2023).

Cyber resilience and risk management. *IEEE Security & Privacy*.

Zhang, Y., et al. (2022).

Artificial intelligence in cloud security. *IEEE Access*.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

