



Task 2 Research issues 3_Critical AI-based detection of cyberattacks in hybrid cloud environments

**Field:
Cybersecurity**

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues(3)

Task 2

ALI MMADI

PhD student - Midocean University

www.midocean.ae

Hello everyone,

In this second assignment, I will present a summary of the main scientific research published in the field of my research project, which falls under Information Technology, with a specialization in cybersecurity.

The topic I have chosen is:

“AI-based detection of cyberattacks in hybrid cloud environments”.

This topic is relevant because organizations are massively migrating to hybrid architectures that combine public cloud, private cloud, and on-premises infrastructures, which increases the complexity of the attack surface.



Summary of major scientific research

Artificial Intelligence and Intrusion Detection Systems (IDS)

Numerous studies have explored the use of Deep Learning to improve intrusion detection systems.

The work of Ian Goodfellow in the field of Deep Learning has demonstrated the ability of neural networks to detect complex patterns in large volumes of data.

Objective of the studies:

Improve the accuracy of network attack detection while reducing false positives.

Methodologies used:

- ☐ Deep neural networks
- ☐ Random Forest
- ☐ Support Vector Machines
- LSTM for temporal analysis

Key results:

- Significant improvement in detection rate
- Better identification of unknown attacks
- Adaptive machine learning capability

Conclusion:

AI significantly enhances the performance of traditional IDS, but remains dependent on the quality of the training data.

In addition, some studies have used the KDD Cup 99 dataset, which is outdated and does not reflect modern threats, limiting the validity of the results.

2. Cloud Computing Security

Research by the National Institute of Standards and Technology has proposed risk management frameworks to secure cloud environments.

Objectives:

Define standards to protect data in virtualized environments.

Methodologies:

- Risk management models
- Vulnerability analysis
- Zero Trust approach

Results:

- ❖ Identification of major threats:
- ❖ Misconfiguration
- ❖ Unauthorized access
- ❖ Insider threats

Cloud security requires a multi-layered approach combining governance, encryption, and continuous monitoring.

3. Detection of Advanced Threats and Zero-Day Attacks

Several recent studies use deep learning models to detect Zero-Day attacks. Research published in IEEE Access and ACM Digital Library shows that LSTM and CNN models improve behavioral detection.

Objective:

Detect unknown attacks not present in traditional databases.

Methodology:

- ☐ Behavioral analysis
- ☐ Unsupervised learning
- ☐ Real-time network traffic analysis

Results:

- ✓ Improved detection capability
- ✓ Reduced response time

Behavioral analysis is more effective than simple signature-based detection.

Main search trends

Based on the analysis of previous studies, several major trends emerge:

◆ 1. Integration of Artificial Intelligence

AI is becoming a central element in modern cybersecurity.

◆ 2. Security in Multi-Cloud Environments

Research focuses on securing hybrid and multi-cloud architectures.

◆ 3. Zero Trust Approach

The Zero Trust model is becoming an emerging standard for access protection.

◆ 4. Behavioral Detection

Shift towards behavioral analysis instead of static signatures.

◆ 5. Automation of Incident Response

Use of SOAR (Security Orchestration, Automation, and Response).

Identified Gaps in the research

Despite significant progress, several gaps remain:

✗ 1. Lack of recent datasets

Many studies still use outdated databases.

✗ 2. Limited real-world experimentation

Models are often tested in lab settings.

✗ 3. Lack of integration between AI and governance

Few studies combine intelligent detection with strategic risk management.

✗ 4. Problem of AI model explainability

Deep Learning models are often seen as “black boxes.”

✗ 5. Few studies targeted at developing countries

The majority of research is conducted in advanced technological environments.

4.Positioning of my research project

My project aims to:

- Propose a hybrid model combining Deep Learning and behavioral analysis
- Test the model in a real hybrid cloud environment
- Integrate an explainability layer (Explainable AI)
- Adapt the solution to critical infrastructure contexts

This project will help fill certain identified gaps, particularly in terms of real-world experimentation and strategic integration.

Conclusion

In conclusion, research in cybersecurity is rapidly evolving towards artificial intelligence, hybrid cloud, and behavioral detection.

However, several challenges remain, including the explainability of models, the lack of real-world validation, and adaptation to specific contexts.

This summary allowed me to place my project within the broader scientific context and clearly identify avenues for innovation.

Thank you for your attention.

KEY REFERENCES

- 1) **Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A.** (2024). *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*. Journal of Big Data.
Publication Date: 04 August 2024.
- 2) **Krishna, R.H., & Selvapriya, B.** (2024). *Comprehensive Review of Intrusion Detection Systems in Cloud Computing*. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 724–731.
Publication Date: 16 March 2024.
- 3) **Abdurrohman & Arainy, C. S.** (2024). *Hybrid Deep Learning Models for Intrusion Detection in Cloud Networks: A Benchmark-Based Comparative Study*. Digitus: Journal of Computer Science Applications, 2(1), 33–42.
Publication Date: 31 January 2024.
- 4) **Joshi, V. R., Assa-Agyei, K., Al-Hadhrami, T., & Qasem, S. N.** (2025). *Hybrid AI Intrusion Detection: Balancing Accuracy and Efficiency*. Sensors, 25(24), Article 7564.
Publication Date: 2025.
- 5) **Mohammed, Y. B., Badara, M. S., & Dan'azumi, H.** (2024). *An Intelligence-Based Cybersecurity Approach: A Review*. Journal of Intelligent Communication, 3(2), 32–43.
Publication Date: September 2024.
- 6) **Baba, M. K., Ya'u, B. I., Zambuk, F. U., Magombe, Y., Musa, M. A., & Alli, A.** (2025). *Artificial Intelligence-Driven Intrusion Detection Systems for Secure Healthcare IoT: A Comprehensive Review*. Impact in Computics, 1(3).
Publication Date: 14 November 2025



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

