



TASK 5 – RESEARCH SKILLS 3

Artificial Intelligence–Based Intrusion Detection and Network Security Performance in Critical Infrastructure

**Field:
Cybersecurity**

Prepared by

ALI MMADI, PhD student-Midocean University



Research Skills (3)

Title of the study:

Artificial Intelligence–Based Intrusion Detection and Network Security Performance in Critical Infrastructure

Variables:

- ☐ **Independent variable:** Artificial Intelligence–Based Intrusion Detection Systems (AI-IDS)
- ☐ **Dependent variable:** Network Security Performance in Critical Infrastructure

Task 5

ALI MMADI

PhD student - Midocean University

www.midocean.ae

السلام عليكم ورحمة الله وبركاته

In this presentation, I will present the title of my research variables and review selected previous studies related to these variables.

According to the methodology of literature review, previous studies must be organized according to the variables of the study. Therefore, the studies will be divided into three groups:

1. Studies related to the first variable: Artificial Intelligence-Based Intrusion Detection Systems.
2. Studies related to the second variable: Network Security Performance in Critical Infrastructure.
3. Studies that combine the two variables together.

This approach helps researchers understand the existing knowledge, identify research gaps, and justify the importance of the proposed research.



1 First: Studies related to the independent variable

Artificial Intelligence-Based Intrusion Detection Systems

Study 1

A study conducted by **Sommer and Paxson (2010)** examined the effectiveness of machine learning techniques in network intrusion detection systems.

The objective of this study was to evaluate how machine learning models can improve the detection of cyberattacks in large network environments.

The researchers used several machine learning algorithms and tested them on real network traffic datasets.

The results showed that machine learning approaches significantly improve the accuracy of detecting cyber threats compared with traditional rule-based detection systems.

However, the study also highlighted limitations such as high computational cost and the need for large training datasets.

Study 2

Another study conducted by **Kim, Lee, and Kim (2016)** investigated the application of deep learning techniques in intrusion detection systems.

The researchers developed a deep neural network model capable of analyzing network traffic patterns and identifying abnormal behaviors.

Their findings indicated that deep learning-based intrusion detection systems achieve higher detection accuracy and lower false alarm rates compared with conventional detection techniques.

The study concluded that artificial intelligence can play a critical role in improving cybersecurity systems in complex digital environments.

Second: Studies related to the dependent variable Network Security Performance in Critical Infrastructure

Study 1

A study conducted by **Ten, Manimaran, and Liu (2010)** analyzed cybersecurity challenges in critical infrastructure systems, particularly in smart grid networks.

The objective of the study was to evaluate how cyberattacks affect the reliability and security performance of critical infrastructure networks.

The results showed that cyberattacks can significantly disrupt communication systems and reduce operational reliability in critical infrastructures.

The study emphasized the importance of implementing advanced security mechanisms to ensure the stability and resilience of critical systems.

Study 2

Another study by **Humayed, Lin, Li, and Luo (2017)** focused on cybersecurity in industrial control systems used in critical infrastructures such as energy and transportation.

The researchers reviewed common vulnerabilities and evaluated different security solutions designed to protect these systems.

The findings revealed that improving cybersecurity mechanisms leads to better system performance, higher resilience, and improved protection against cyber threats.

The study recommended integrating advanced detection and monitoring technologies in critical networks.

Third: Studies combining the two variables

Combined Study

A study conducted by **Shone, Ngoc, Phai, and Shi (2018)** examined the use of deep learning-based intrusion detection systems to enhance network security.

The researchers proposed a deep learning architecture designed to detect sophisticated cyberattacks in large-scale network environments.

Their results demonstrated that artificial intelligence-based intrusion detection systems significantly improve network security performance by detecting attacks earlier and reducing response time.

The study concluded that integrating artificial intelligence techniques into cybersecurity frameworks is essential for protecting modern digital infrastructures.

In conclusion, the review of previous studies shows that artificial intelligence technologies have become an essential tool in cybersecurity.

Previous research has demonstrated that AI-based intrusion detection systems improve the accuracy and efficiency of detecting cyber threats, while strong cybersecurity mechanisms improve the performance and resilience of critical infrastructure networks.

However, there is still a need for further research to explore how artificial intelligence can be optimized to protect critical networks more effectively, particularly in developing digital environments.

Therefore, the proposed research aims to further investigate the relationship between artificial intelligence-based intrusion detection systems and network security performance in critical infrastructures. **Thank you for your attention ,Wa Billahi Tawfiq.**

Reference Frameworks

- 1) Robin Sommer & Vern Paxson (2010).
Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.
In Proceedings of the IEEE Symposium on Security and Privacy.
<https://doi.org/10.1109/SP.2010.25>
- 2) Jong Hyuk Kim, Jae Hoon Lee & Kwangjo Kim (2016).
Deep Learning-Based Intrusion Detection System for Cyber Security.
- 3) Chee-Wooi Ten, Govindarasu Manimaran & Chen-Ching Liu (2010).
Cybersecurity for Critical Infrastructures: Attack and Defense Modeling for the Smart Grid.
IEEE Transactions on Smart Grid
- 4) Alaa Humayed, Jinjun Lin, Fengjun Li & Bo Luo (2017).
Cyber-Physical Systems Security—A Survey.
IEEE Internet of Things Journal



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

