

Course: Research Methodology (A100)
Assignment Two: Problem Statement and Research Objectives
Research Title: Detecting Cyber Attacks Using Artificial Intelligence
Prepared by Student: Rahaf Alsaiari
Faculty Member: Dr. Mohammed Anbar

Table of Contents

Problem Statement	1
Components of the Problem Statement	2
2.1 Identifying the Problem	
2.2 Describing the Problem	
2.3 Importance of the Problem	
2.4 Current Solutions	
2.5 Limitations of Current Solutions	
Research Objectives	3
References	4

1. Problem Statement

In recent years, the digital infrastructure has witnessed significant expansion, making reliance on electronic systems and services an essential part of the operations of governmental and private institutions. With this expansion, more complex and advanced cyberattacks have emerged, relying on new methods that are difficult for traditional security systems to handle, especially those based on fixed rules or signatures of previous attacks.

At the same time, traditional intrusion detection systems face major challenges, such as high false alarm rates, weak ability to detect modern attacks (Zero-day Attacks), in addition to their inability to process and analyze the massive data generated by modern systems such as cloud services and the Internet of Things.

On the other hand, artificial intelligence technologies—especially machine learning and deep learning—offer better capabilities for analyzing network behavior and recognizing abnormal patterns. Despite this advantage, their application in real-world environments faces challenges related to limited data, difficulty in generalization, and the need for high computational power for some models.

Accordingly, the research problem is:

'The limitations of traditional security systems in detecting modern cyber attacks, and the need to study and evaluate the role of artificial intelligence technologies in improving the accuracy and speed of detection systems in real-world environments.'

2. Components of the Problem Statement

2.1 Problem Identification

The increasing complexity of cyberattacks versus the limited ability of traditional systems to detect new and evolving patterns.

2.2 Problem Description

Traditional systems rely on fixed rules or signatures, making them ineffective against modern and previously unknown attacks, especially in environments with large and dynamic data.

2.3 Importance of the Problem

Protecting sensitive data and reducing financial losses.

Supporting secure digital transformation within organizations.

Reducing the rate of successful attacks.

Improving national and global cybersecurity levels.

2.4 Current Solutions

Traditional Intrusion Detection Systems (IDS).

Basic machine learning algorithms.

Systems relying on outdated attack databases.

2.5 Limitations of Current Solutions

Inability to detect new attacks.

High false alarm rates.

Poor performance with big data.

Difficulty in generalizing to different environments.

3. Research Objectives

Main Objective

To analyze the effectiveness of artificial intelligence techniques in improving the performance of cyberattack detection systems compared to traditional methods.

Sub-objectives (Research Objectives)

- To identify the different AI-based techniques used in detecting cyberattacks.
- To compare ML and DL algorithms in terms of accuracy, speed, and efficiency.
- To evaluate the generalization of AI models using real-world datasets.
- To examine limitations such as data imbalance, model interpretability, and overfitting.
- To propose future research directions that enhance AI-based detection systems.
- To explore the impact of hybrid and ensemble models on improving detection accuracy.

References

(Andrea Pinto, Luis-Carlos Herrera, Yezid Donoso, Jairo A. Gutierrez.2023). A Survey on Intrusion Detection Systems Based on Machine Learning. Sensors, 23(5), 2415. <https://www.mdpi.com/1424-8220/23/5/2415> (Zhiwei Xu, Yujuan Wu, Shiheng Wang, Jiabao Gao, Tian Qiu, Ziqi Wang, Hai Wan, Xibin Zhao. 2025). Deep Learning-based Intrusion Detection Systems: A Survey. arXiv preprint. <https://arxiv.org/abs/2504.07839> (MM Rahman, S Al Shakil, MR Mustakim. 2024). Survey on Intrusion Detection System in IoT Networks. ScienceDirect. <https://www.sciencedirect.com/science/article/pii/S2772918424000481> (Md Alamin Talukder, Md Manowarul Islam, Md Ashraf Uddin, Khondokar Fida Hasan, Selina Sharmin, Salem A. Alyami, Mohammad Ali Moni. 2024). Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Datasets. Journal of Big Data. <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00886-w> (Sunday Adeola Ajagbe, Joseph Bamidele Awotunde, Hector Florez.2024). Intrusion Detection: A Comparison Study of Machine Learning Models. SN Applied Sciences. <https://link.springer.com/article/10.1007/s42979-024-03369-0> (Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, Kashif Kifayat. 2020). A Comprehensive Survey of AI-Enabled Phishing Attack Detection Techniques. Telecommunication Systems. https://www.researchgate.net/publication/344583507_A_comprehensive_survey_of_AI_enabled_phishing_attacks_detection_techniques