AI-Driven Hybrid Cyber Defensive System for Intelligent Malware Detection and Threat Insight

1 Introduction

1.1 Overview

The proposed project is an AI-Based Intelligent Cyber Defensive Tool that integrates Malware Detection with NLP for Threat Intelligence Insights. The system will use a hybrid AI model combining machine learning (ML) and deep learning (DL) techniques to enhance cybersecurity defenses. The primary goal of the project is to detect, analyze, and mitigate cyber threats proactively. The tool will function as an advanced cybersecurity assistant, helping organizations prevent and respond to cyberattacks in real time. Key features include AI-powered malware detection, NLP-driven threat intelligence, behavioral analysis, automated response mechanisms, and Explainable AI (XAI) for decision-making transparency.

1.2 SGD goal

This project aligns with multiple SDGs by strengthening digital infrastructure security (Goal 9), protecting institutions from cybercrime (Goal 16), and promoting cybersecurity education (Goal 4). By developing a robust AI-based cyber defense system, it contributes to a safer digital environment, reduces cyber threats, and fosters cybersecurity innovation.

2 Literature Review

Kim et al. (2021) proposed a deep learning-based malware detection framework using behavioral analysis. The proposed tool builds on this concept by integrating NLP for real-time threat intelligence. Zhang et al. (2022) explored NLP for cyber threat intelligence extraction, which we enhance by combining it with AI-driven threat detection. This research serves as a foundation for developing a comprehensive AI-based cybersecurity solution.

3 Methodology

3.1 Dataset

The dataset for this project will include Malware Samples collected from public sources such as VirusTotal, MalwareBazaar, and cybersecurity research repositories, ensuring a rich dataset with both malware and benign samples. It will have CSV for structured logs, JSON for threat intelligence feeds, and text for NLP processing.

3.2 Approach

The hybrid deep learning model integrates multiple techniques for enhanced threat detection, including CNNs or RNNs for malware classification, transformer models (e.g., BERT) for NLP-based threat intelligence, and LSTMs or autoencoders for behavioral anomaly detection.