Project Title

(Educational AI-Based Network Intrusion Detection System (IDS

Prepared by 🔹

Abdulrahman Khaled Mohammed Haggam
Country: Yemen

Introduction .1 🔹

Network intrusion detection systems (IDS) play a critical role in identifying malicious activities and protecting digital infrastructures. However, many traditional IDS solutions rely on static .signatures, making them less effective against evolving cyber threats

This project presents an educational AI-based Intrusion Detection System designed to monitor simulated network traffic and detect intrusion attempts using machine learning techniques. The system focuses on safe, ethical, and academic experimentation, making it .suitable for cybersecurity learning and research

---

Objectives .2 🔹

Design an educational AI-based intrusion detection system

Detect malicious and abnormal network behavior

Apply machine learning techniques in cybersecurity defense

Demonstrate safe and ethical cybersecurity experimentation

Support learning and academic research in cybersecurity

Methodology .3 🔹

Data Collection 3.1

Publicly available network intrusion datasets were used to simulate network traffic, including .normal and attack scenarios. No real systems or users were involved

Data Processing 3.2

Data cleaning and normalization

Feature selection relevant to network behavior

Labeling traffic as normal or intrusion

Preparing data for model training

Machine Learning Models 3.3

:The following models were implemented

Random Forest

(Support Vector Machine (SVM

.to identify intrusion patterns within network traffic

System Implementation 3.4

The IDS was implemented in a simulated and offline environment to evaluate detection .performance safely and ethically

Evaluation 3.5

:Performance was measured using

Detection accuracy

Intrusion detection rate

False positive rate

🔹 Expected Results .4

Accurate identification of intrusion attempts

Reduced false alerts compared to traditional IDS

Faster response to suspicious traffic

Clear demonstration of AI-driven intrusion detection

🔹 5. Tools and Technologies Used

Programming Language: Python

Machine Learning: scikit-learn, TensorFlow

Environment: Simulated educational environment

(Operating System: Linux (Ubuntu

🔹 6. Results and Achievements

Analyzed over 20,000 simulated network traffic records

Detected approximately 92–95% of intrusion attempts

Reduced false positives by 30–40%

Demonstrated practical AI-based IDS concepts

🔹 7. Impact and Significance

This project demonstrates the practical application of AI in intrusion detection and highlights its importance in modern cybersecurity defense systems. It serves as a strong educational foundation for advanced cybersecurity studies.

🔹 8. Connection to Future Studies and Career Goals

This project aligns with my academic goal of specializing in cybersecurity, particularly in threat detection, network security, and AI-driven defense mechanisms.

🔹 Ethical Considerations

All experiments were conducted in simulated environments using public datasets, following ethical cybersecurity standards.

—