AI-Based Intrusion Detection System

Hybrid Machine Learning Approach Combining LSTM, Random Forest & SVM for Enhanced Cybersecurity

1. Introduction:

Cybersecurity threats are evolving rapidly, making traditional signature-based intrusion detection systems (IDS) inadequate.

This project proposes a hybrid AI-based IDS that leverages the strengths of LSTM (deep learning), Random Forest (ensemble learning),

and SVM (margin-based learning) to detect network intrusions with high accuracy.

2. System Architecture:

Components:

- Data Collection Module: Gathers network traffic (e.g., NSL-KDD or CICIDS datasets).
- Preprocessing Module: Handles feature extraction, normalization, and encoding.
- Hybrid Model Module:
- LSTM for temporal analysis of traffic sequences.
- Random Forest for robust classification and noise handling.
- SVM for boundary-based detection of anomalies.
- Fusion Module: Combines predictions via ensemble techniques (e.g., majority voting or weighted average).
- Alert System: Notifies on detected intrusions via logs or dashboards.
- Evaluation Module: Measures performance using accuracy, precision, recall, F1-score, ROC-AUC.

3. Workflow:

1. Input: Raw network traffic data.
2. Data preprocessing and transformation.
3. Parallel training and prediction by LSTM, RF, and SVM.

4. Ensemble fusion for final classification.

5. Output: Intrusion or normal behavior alert.

4. Key Features:

- Real-time or batch processing.

- High detection accuracy with reduced false positives.

- Adaptable to various network topologies.

- Scalable for large datasets.

5. Technologies Used:

- Languages: Python (TensorFlow, Scikit-learn, Keras, NumPy, Pandas)

- Tools: Jupyter Notebook, Wireshark, Matplotlib, Docker (optional)

- Datasets: NSL-KDD, CICIDS 2017/2018

6. Use Cases:

- Enterprise-level network security monitoring.

- Cloud infrastructure intrusion detection.

- Smart IoT security systems.