Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment

The increasing use of IoT devices has led to a rise in security vulnerabilities, particularly botnet attacks. This project proposes a hybrid machine learning approach to effectively detect such threats using advanced preprocessing techniques and neural attention layers to improve detection accuracy and performance.

Tools & Libraries Used: - Python - Pandas, NumPy for data handling - Matplotlib for data visualization - Scikit-learn for preprocessing and traditional ML methods - Keras for deep learning model with attention layer

Dataset: A publicly available IoT botnet traffic dataset was used. It includes various traffic features labeled as benign or botnet-infected.

Methodology: 1. Data Cleaning and Encoding using LabelEncoder 2. Standardization with StandardScaler 3. Splitting dataset into training and testing sets 4. Applying Hybrid Neural Network with Attention Layer to enhance focus on important features 5. Evaluation of model accuracy, precision, recall, and F1-score

Results: The proposed model achieved high accuracy and robustness in detecting botnet attacks, outperforming traditional machine learning methods through the integration of attention mechanisms.

Conclusion: This hybrid approach demonstrates the potential of combining classical and deep learning methods with attention for real-time botnet detection in IoT networks.