Real-Time Detection of DDoS Attacks Using Lightweight Neural Networks and Machine Learning Classifiers

Group - 1

Project Objectives

- **Detect and mitigate DDoS attacks using intelligent models**
- **Compare traditional classifiers with deep learning approaches**
- **Enable real-time inference suitable for edge devices**

Dataset Description

Dataset : CIC-DDoS 2019 dataset

Contains over 31 million records across various attack types. A sampled, preprocessed subset was used for training, with a 60:40 benign-to-malicious ratio.

Model Architecture

- Shallow Neural Network (Edge-optimized)
- Naïve Bayes, DT, SGD, KNN, SVM, Random Forest, XGBoost, QDA

Evaluation metric : Accuracy Score

System Architecture

Data Collection → Preprocessing → Model Inference → Detection

Best Models by Accuracy

Neural Network (99.14%)	XGBoost (97.91%)
SVM (96.94%)	KNN (96.24%)

Key Findings

- SNN captured complex patterns and scaled well for real-time detection.
- XGBoost and SVM handled noise and non-linearity effectively.
- KNN was simple but costly at inference, limiting real-time use.

Key Contributions

- Developed a lightweight, high-accuracy DDoS detection model
- Demonstrated feasibility of edge deployment
- Showcased real-time detection with minimal latency

Conclusion

Adaptive ML models improve DDoS detection. Our shallow neural network offers high accuracy with low overhead, ideal for real-time use.