**Project Report Summary: IoT Intrusion Detection System (IDS) with Adversarial Training**

Objective

The project develops a lightweight Intrusion Detection System (IDS) tailored for IoT devices, specifically optimized for deployment on Raspberry Pi 4/5 (ARM64 architecture). The system incorporates adversarial training using the Projected Gradient Descent (PGD) attack to enhance robustness against adversarial examples. The solution is designed to process IoT network traffic data efficiently, detect anomalies, and export a model optimized for edge deployment.

Brief Description

Hardware Optimization :

The system is optimized for resource-constrained environments like Raspberry Pi by reducing batch size (BATCH\_SIZE=64) and designing a lightweight neural network architecture.

The model is exported in TorchScript format for efficient ARM-based deployment.

Data Preparation :

The script uses the N-BaIoT dataset, which contains preprocessed IoT network traffic data.

Features are normalized using StandardScaler to ensure consistent input scaling for the neural network.

A temporal validation split ensures that the model evaluates performance on unseen future data.

Lightweight Neural Network :

A compact neural network (IoTIDSModel) is implemented with three fully connected layers, ReLU activations, and dropout for regularization.

The architecture balances accuracy and computational efficiency, making it suitable for edge devices.

Adversarial Training :

The PGD attack generates adversarial examples during training, improving the model's robustness to adversarial inputs.

Combined loss (clean + adversarial) ensures the model learns from both normal and perturbed data.

Edge Deployment :

The trained model is exported as a TorchScript file (iot\_ids\_model.pt) for deployment on ARM processors.

A separate inference script is provided for real-time predictions on Raspberry Pi.

IoT-Specific Features :

Temporal validation ensures the model generalizes well to future network traffic patterns.

Lightweight architecture and feature engineering make the system suitable for IoT-specific use cases.

Outcomes

Adversarial Robustness :

The inclusion of PGD adversarial training enhances the model's ability to handle adversarial attacks, a critical requirement for IoT security.

Efficient Edge Deployment :

The TorchScript export enables seamless integration with edge devices, ensuring low-latency inference.

Scalability :

The lightweight architecture and hardware optimization make the system scalable for deployment across multiple IoT devices.

Real-Time Monitoring :

The system can be extended with MQTT integration for real-time monitoring and anomaly detection in IoT networks.

Key Insights

Adversarial Training Benefits :

Adversarial training improves the model's resilience to adversarial examples, reducing false negatives in high-stakes IoT environments.

Hardware Constraints :

Reducing batch size and model complexity ensures compatibility with Raspberry Pi's limited memory and processing power.

Temporal Validation :

Using a temporal split for training and testing ensures the model evaluates performance on realistic, time-ordered data.

Edge Deployment :

Exporting the model in TorchScript format simplifies deployment on ARM-based devices and enables integration with C++ applications via libtorch.

Conclusion

This project demonstrates the development of a robust and efficient IoT IDS optimized for deployment on edge devices like Raspberry Pi. By incorporating adversarial training and hardware-specific optimizations, the system addresses key challenges in IoT security, such as resource constraints and vulnerability to adversarial attacks. The solution provides a foundation for real-time anomaly detection in IoT networks, with potential extensions for production-grade deployment.