# BUILDING AN INTELLIGENT EDGE SECURITY GATEWAY FOR IOT MALWARE DETECTION USING DEEP NEURAL NETWORKS

**Đỗ Đình Vạn**[1]

[1] University of Information Technology, Ho Chi Minh City, Vietnam

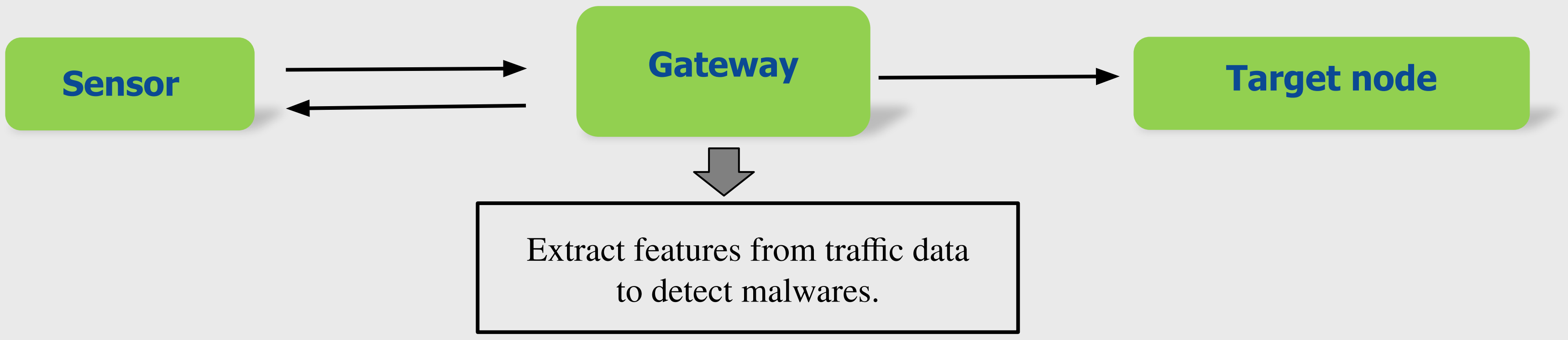
## What ?

- An Intelligent Edge Security Gateway for IoT We developed a low-cost, real-time Intrusion Detection System deployed directly on a Raspberry Pi to protect vulnerable IoT networks.

## Why ?

- IoT Vulnerabilities: Billions of IoT devices lack robust security, making them easy targets for Botnets (e.g., Mirai) to launch massive DDoS attacks.
- Latency Issues: Sending data to the Cloud for security analysis creates significant delays, preventing immediate threat blocking.
- Resource Constraints: Traditional AI models are too heavy for edge devices, while standard firewalls fail to detect complex, dynamic attack patterns.

## Architecture



Sensor

Gateway

Target node

Extract features from traffic data to detect malwares.

## Description

### 1. Gateway data flow

- **Traffic Interception:** The Raspberry Pi captures raw network packets passing through the gateway.
- **Feature Extraction (Zeek): Zeek** converts raw packets into compact connection logs (conn.log), extracting key flow metadata (Time, Duration, Payload Size, State).
- **Preprocessing & Inference:** A Python module reads logs in real-time, applies **Standard Scaling**, and feeds data into the AI model.
- **Detection & Response:** The AI predicts **Benign** vs. **Malicious**. If Malicious ($P > 0.5$), an alert is triggered immediately.

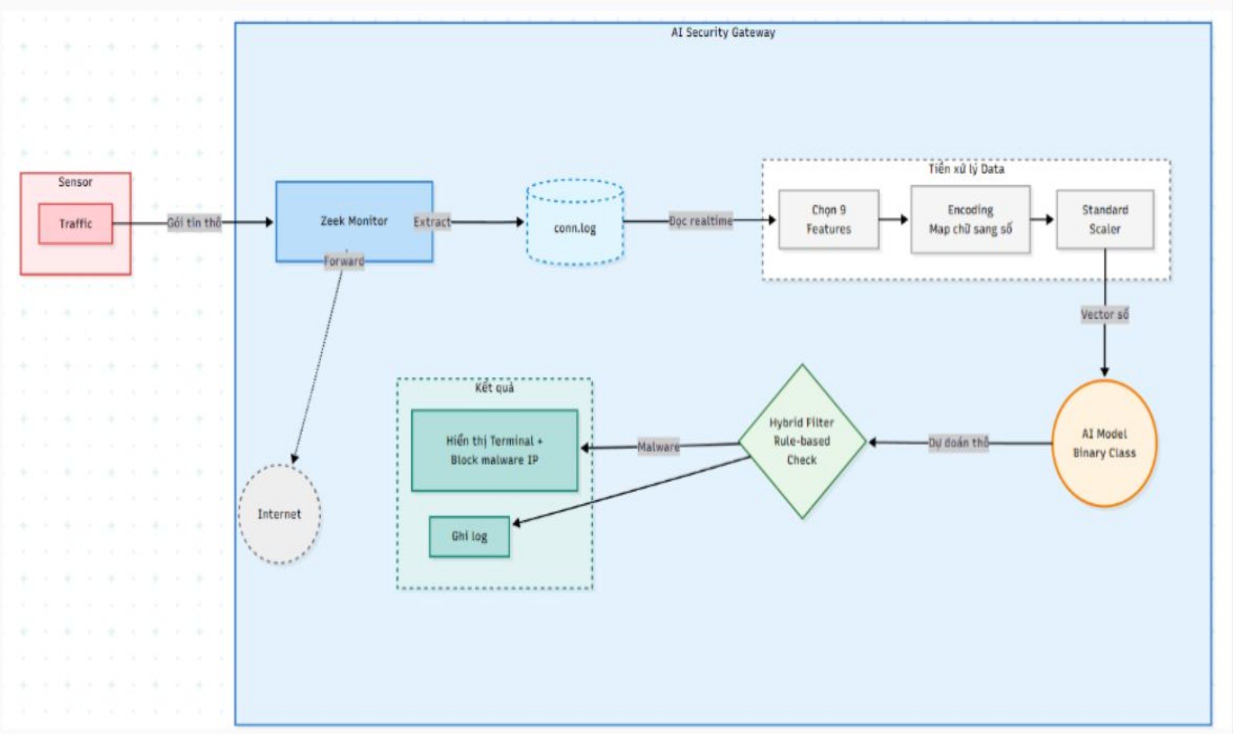


***Figure***. Data flow diagram

### 2. The AI Model in gateway

A **Lightweight Deep Neural Network (DNN)** optimized for edge devices with limited resources.

- **Architecture:** Feed-forward MLP with a "Funnel" structure to compress features.
- **Optimization:** Uses **ReLU** activation for speed and **Dropout (0.5)** to prevent overfitting.
- **Performance:** Ultra-fast inference time (**< 10ms**) suitable for real-time filtering.

**NII** **Tên tác giả chính– Trường Đại học**
**TEL : *********** **Email : ***********