Technical Datasheet: Raspberry Pi 5 Hotspot Project

# 1. Overview

This technical datasheet outlines the steps and components involved in creating a fully functional and secure WiFi and Bluetooth hotspot using a Raspberry Pi 5. The project includes network filtering, IP/MAC address management, firewall configuration, and options to integrate AI-based monitoring for enhanced security.

# 2. Hardware Requirements

The project requires the following hardware components:

- Raspberry Pi 5 (or Raspberry Pi 4 for alternative setups)  
- USB WiFi adapter (if not using onboard WiFi)  
- Bluetooth dongle (if needed)  
- Hailo-8L AI Accelerator (optional for advanced AI features)  
- MicroSD card (32 GB or higher)  
- Ethernet cable (for wired connections)  
- Power supply for Raspberry Pi 5

# 3. Software and Packages

The following software and packages are required to set up the hotspot, network monitoring, and filtering:

- Raspberry Pi OS (Lite or Desktop version)  
- hostapd (to create WiFi access point)  
- dnsmasq (for DHCP services)  
- iptables (for firewall and IP/MAC filtering)  
- bluez (for Bluetooth management)  
- fail2ban (for monitoring and banning IPs)  
- arpwatch (to monitor MAC addresses)  
- nmap (for network device scanning)  
- Optional: Hailo-8L drivers and SDK (for AI acceleration)

# 4. Setup and Configuration

## 4.1 System Update and Driver Installation

Update the system and install the necessary drivers for managing network interfaces (USB, WiFi, and Bluetooth).

Commands:  
```bash  
sudo apt update && sudo apt upgrade -y  
sudo apt install usb-modeswitch ethtool hostapd dnsmasq iptables python3 bluetooth bluez -y  
```

## 4.2 Creating a Secure WiFi and Bluetooth Access Point

Configure the Raspberry Pi as a secure WiFi and Bluetooth hotspot. The configuration involves setting up hostapd for WiFi access and bluez for Bluetooth. This section covers the key configuration files and service management.

## 4.3 Network Filtering and IP/MAC Management

This section focuses on how to filter traffic using iptables and manage IP and MAC addresses for security. Blocking suspicious or unauthorized devices can be done through both IP and MAC filtering.

## 4.4 Firewall Configuration (iptables)

iptables is configured as the main firewall to control incoming and outgoing traffic. The firewall rules should be configured to block all unauthorized access while allowing key services like SSH and HTTP.

Commands:  
```bash  
sudo iptables -F  
sudo iptables -P INPUT DROP  
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT # SSH  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP  
```

# 5. Monitoring and Security Enhancements

## 5.1 Fail2Ban and arpwatch

Fail2Ban monitors authentication logs and bans IP addresses with suspicious activity. arpwatch is used for MAC address monitoring to detect devices that connect to the network. Together, these tools enhance security by detecting and reacting to threats in real-time.

## 5.2 AI-Driven Network Monitoring (with Hailo-8L)

With the Hailo-8L AI accelerator, advanced AI-driven network monitoring and filtering can be implemented. This allows for anomaly detection, predictive threat analysis, and deep packet inspection (DPI) for enhanced security.

# 6. Optional Enhancements

- \*\*Hailo-8L AI integration\*\*: Add advanced AI features for predictive network analysis and threat detection.  
- \*\*VPN integration\*\*: Secure the hotspot traffic further with a VPN solution such as WireGuard or OpenVPN.  
- \*\*Network segmentation\*\*: Create isolated network zones for different types of devices (IoT, guests, etc.).

# 7. Conclusion

This Raspberry Pi 5 Hotspot Project provides a comprehensive solution for setting up a secure, manageable, and scalable network access point. Whether using it for personal, business, or IoT purposes, the system ensures security with advanced filtering, monitoring, and AI-based features for a highly secure network environment.