**NET SENTINELS**

**🛠️ Problem Statement (100–150 words)**

As of 2024, there are over **17 billion connected IoT devices** worldwide — from smart locks to industrial sensors. Unfortunately, most of these devices have **little to no security**, often using hardcoded credentials, outdated firmware, or weak encryption. According to Kaspersky, **1.5 billion IoT attacks** were detected in H1 2023 alone. Traditional security solutions rely on centralized firewalls or cloud-based monitoring, which create single points of failure and don’t scale with the complexity of home and enterprise IoT networks. Once compromised, a single smart plug or camera can become a launchpad for **botnets, ransomware, or lateral movement within a network**. The current ecosystem lacks a scalable, self-regulating, and decentralized solution to this growing threat.  
**Beginner-friendly tech stack (exact tools)**

* **Language:** Python (everyone on the team uses the same language)
* **Messaging (devices talk):** MQTT with **Eclipse Mosquitto** broker or **ZeroMQ (pyzmq)**
* **Anomaly detection:** **Scikit-learn** IsolationForest or **PyOD** library (easy outlier detection)
* **Dashboard/UI:** **Streamlit** (fast to build a UI with Python only)
* **Storage/Log:** JSON files or **SQLite** via Python sqlite3

**Simple architecture (text diagram)**

* Multiple **Device processes** (Python scripts)  
  ↕ (publish/subscribe)
* **Local MQTT broker** (Mosquitto) or **ZeroMQ hub**  
  ↕
* **Coordinator/Quorum service** (Python process logs votes)  
  ↕
* **Streamlit Dashboard** (reads logs/DB and shows device states)