GuardianNode: Agentic AI for IoT Security & F3P Monitoring

Agentic AI–driven, privacy-first IoT security gateway with real-time behavioral monitoring without firmware access. Designed for heterogeneous, vendor-neutral IoT ecosystems.

The Real Problem

Why IoT Security is Fundamentally Broken

Silent Data Exfiltration

IoT devices silently exfiltrate encrypted data

Impossible at Scale

Manual flow analysis is impossible at scale

Zero Visibility

No visibility into latency abuse, endpoint churn, or attack origin

Privacy Violations

Existing DPI-based or firmware solutions violate privacy or break devices

Core Objective: Privacy-First, Deterministic Control

Design Objective

Secure IoT without breaking encryption.

Treat all devices as untrusted by default.

- **Secure IoT without breaking encryption**
- **Treat all devices as untrusted by default**
- **Enforce behavior at the network layer, not the device**
- **Keep ownership local — no cloud dependency**

GuardianNode: How the System Works

Solution Overview

01

Agentic AI Reasoning Layer

Agentic AI reasoning layer for detection & policy decisions

02

Hardware-Assisted Enforcement

Hardware-assisted enforcement for guaranteed isolation

03

Continuous Learning

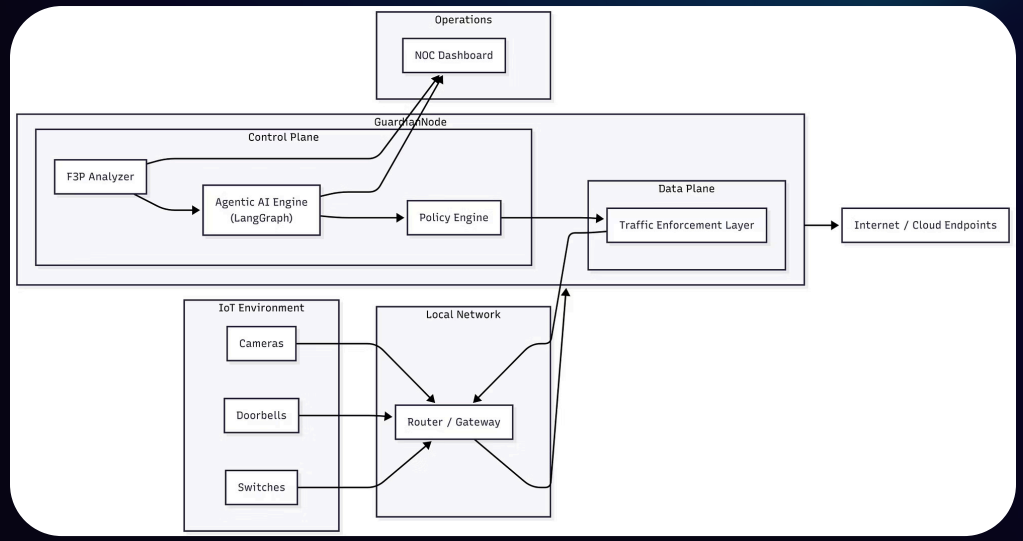
Continuous learning of "normal" device behavior

04

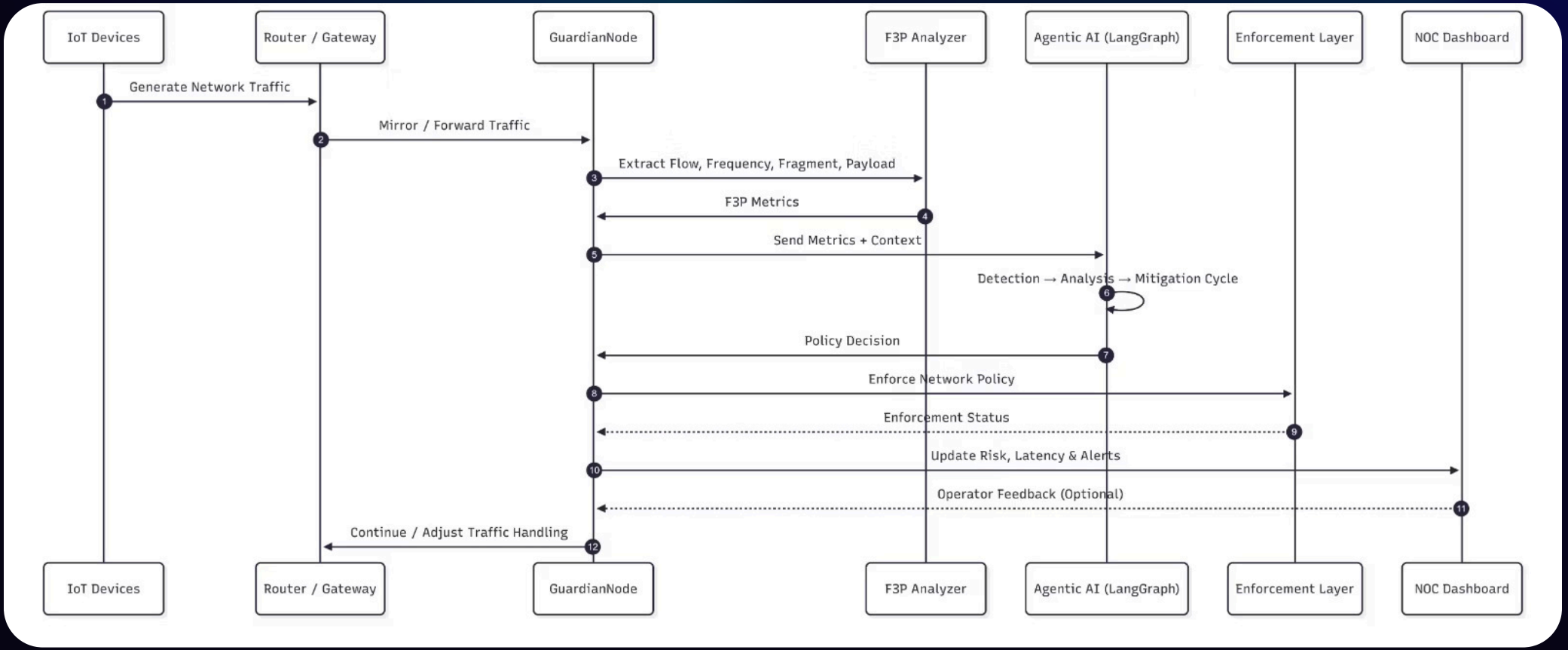
Real-Time Visualization

Real-time visualization via NOC dashboard

Architecture Diagram



Sequence-row Diagram



Where GuardianNode Lives in the Network

Hardware & Network Topology

IoT devices → Router → GuardianNode → Internet

1

Deployed at router / local gateway layer

2

Sees all device traffic without device modification

3

Works for cameras, switches, doorbells, sensors

4

Suitable for home, enterprise, and industrial networks

Deterministic Enforcement Using NoC Principles

NoC-Based Parallel Traffic Isolation

- Each IoT device mapped to a dedicated hardware pipeline
- Lightweight on-chip routing fabric (NoC-inspired)
- Parallel, interference-free policy enforcement
- Guarantees isolation even under attack conditions

> Multiple parallel pipelines (NoC-style blocks) — One pipeline per device

F3P: Flow, Frequency, Fragment, Payload

The F3P Framework

Four analytical lenses converging to a risk score

Flow

Destination endpoints, geolocation, routing patterns

Frequency

Burst rate, idle-time activity, periodic beacons

Fragment

Packet size variance, fragmentation anomalies

Payload

Metadata patterns (without decryption)

Enables latency detection and attack vector identification

How GuardianNode Identifies Threats

Latency & Attack Detection

Abnormal RTT Detection

Detects abnormal RTT and jitter per device

Geolocation Correlation

Correlates latency with endpoint geolocation

Threat Identification

Identifies DDoS participation, C2 beaconing, misconfigured firmware

Encrypted Payload Support

Works even with encrypted payloads

Why We Use Agentic AI (Not Static Rules)

Agentic AI Architecture

Built using LangGraph

- Stateful multi-agent system
- Agents specialize in detection, analysis, mitigation, explanation
- Policies evolve with device behavior

Multi-agent loop diagram with state memory between cycles

Detection

Analysis

Mitigation

Explanation

Detection → Analysis → Mitigation (Closed Loop)

LangGraph Cycles Explained

Detection Agent

Monitors F3P metrics continuously

Analysis Agent

Compares against learned baseline

Mitigation Agent

Adjusts rate, priority, isolation

Memory State

Preserves historical context across cycles

Cyclic state machine diagram

Hardware-Software Co-Design

Control Plane vs Data Plane

Data Plane (FPGA):

- Line-rate packet classification
- Rate limiting & isolation

Control Plane:

- Agentic reasoning
- Policy orchestration
- Risk scoring

Network Operations Center (NOC) View

NOC Dashboard Integration

- Real-time device visibility
- Per-device risk and latency metrics
- Visual attack source geolocation
- Human-readable AI explanations

Dashboard with device cards, risk scores, maps

Security Without Surveillance

Privacy-First Enforcement Model

No firmware modification

No payload decryption

No vendor cloud dependence

Enforcement via shaping, prioritization, time-based control

Why GuardianNode Matters

Innovation & Impact

- Vendor-neutral by design
- Scales from homes to telecom networks
- Aligns with national cybersecurity & digital trust goals
- Practical, deployable, and explainable

Home → Enterprise → Nation scale icons

Conclusion

Key Points:

- **Restores user control over IoT data**
- **Detects threats without breaking privacy**
- **Combines deterministic hardware with adaptive intelligence**

Surendar P VIT Chennai

Ashwath P SRM-Ramapuram

Vamsi Krishna VIT Chennai

Experience: currently interning at Nokia solutions and networks