BMS INSTITUTE OF TECHNOLOGY & MANAGEMENT

CODE RED 25

CODE TILL YOU DROP...

SOLUTION OUTLINE

Problem Statement: Autonomous Cybersecurity for Real-Time IoT Node Protection
Problem Statement Code: CR06
Team Name: Unicorn
Team Leader Name : Prabu Jayant

CODE RED '25

IDEA/APPROACH DETAILS

IDEA/SOLUTION - GUARDIAN MESH

Intelligent security mesh using **containerized nodes** with ML-driven threat detection and automated recovery, ensuring critical service continuity during cyber attacks through **instant backup activation** and **federated learning**. The Guardian Mesh redefines IoT cybersecurity with the first fully autonomous security framework designed for real-time (<1s) threat detection and mitigation. This system employs an **AI-driven zero-trust architecture,** ensuring that no data is shared between nodes, thus minimizing the attack surface.

UNIQUE VALUE PROPOSITION

- **Real-Time Response:** Mitigates threats in under one second for seamless IoT operations.
- **Zero-Trust Security:** Prevents vulnerabilities with no inter-node data sharing.
- **Self-Healing Network:** Restores nodes 60% faster with automated failover.
- **Scalable Design:** Adapts to any IoT ecosystem without hardware changes.
- **Continuous Improvement:** Enhances defences via federated learning without data exposure.

Product Status: 70% product is completed and further build is in progress.

Channels: Govt. schemes, industries, organizations etc.

USE CASES

- **Smart Cities:** Secures traffic systems and grids from cyberattacks.
- **Healthcare IoT:** Protects medical devices and patient data.
- **Industrial IoT:** Safeguards factories and supply chains from breaches.
- **Smart Homes:** Shields home devices for privacy and safety.
- **Critical Infrastructure:** Defends utilities and networks against cyber threats.

IDEA/APPROACH DETAILS

Tech Stack used

- **Docker**: to deploy our framework in a multi node docker environment to simulate detection, isolation and recovery.
- **Python**: used python to write scripts for getting node network health and to implement ML model for network anomaly detection
- **Scikit-Learn**: Library for Isolation Forest implementation to detect anomalies.
- **React:** web interface to visualize iot node network in real time.
- **Flask**: used for backend communications from the nodes to the web interface.
- **Zero-Trust Architecture:** this architecture enforces independent node operations, to enhance security minimizing possible of risk from spreading.

Showstopper Features

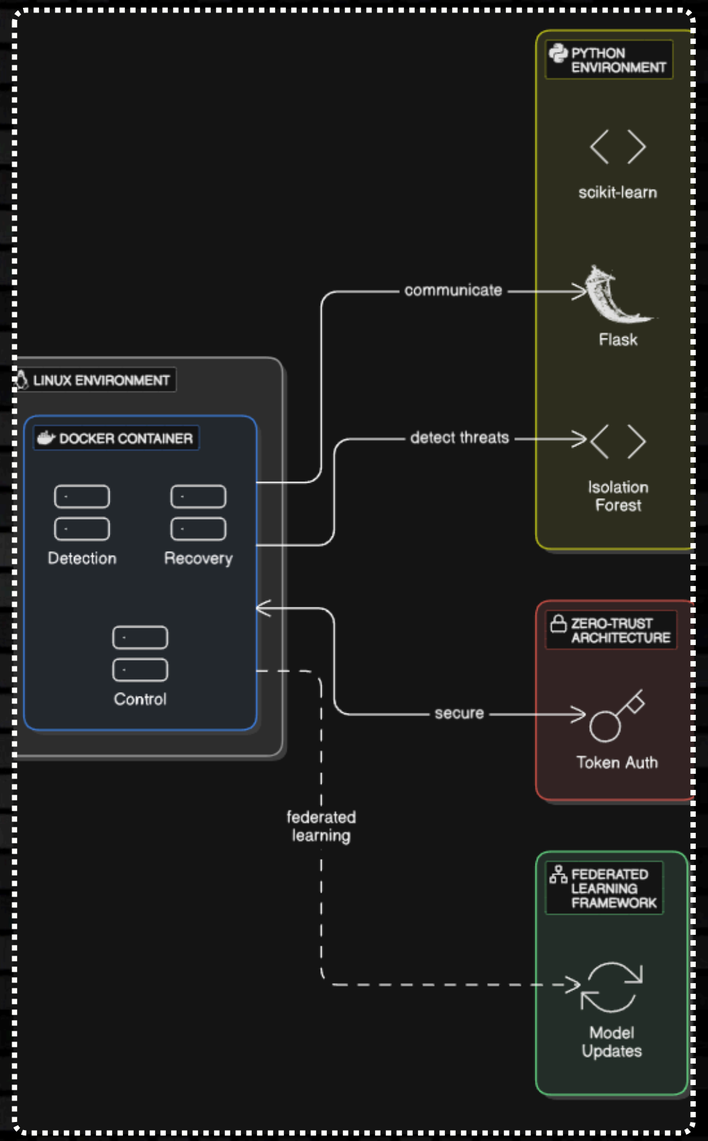
- **Threat Prevention:** Isolates compromised nodes to prevent threats and maintain network integrity using ML detection.
- **Accountability:** Enables auditing of flagged nodes with detailed records for security refinement.
- **Minimal Disruption:** Ensures service continuity by isolating anomalies, restricting communication, and activating secure backups.
- **User-Centric Interface:** Simplifies security workflows with an intuitive dashboard experts.

Isolation Forest(ML)

- **Feature Extraction:** Extracts byte size, MAC addresses, ports, and protocol data to create a feature set for anomaly detection.
- **Unsupervised Learning:** Learns normal traffic patterns without labeled data by isolating outliers using binary trees.
- **Anomaly Scoring:** Calculates anomaly scores based on ethernet packet information like port number, byte length MAC etc , identifying abnormal or unusual traffic patterns.
- **Real-Time Action:** Enables continuous detection and triggers automated isolation or logging for anomalous nodes in real time.

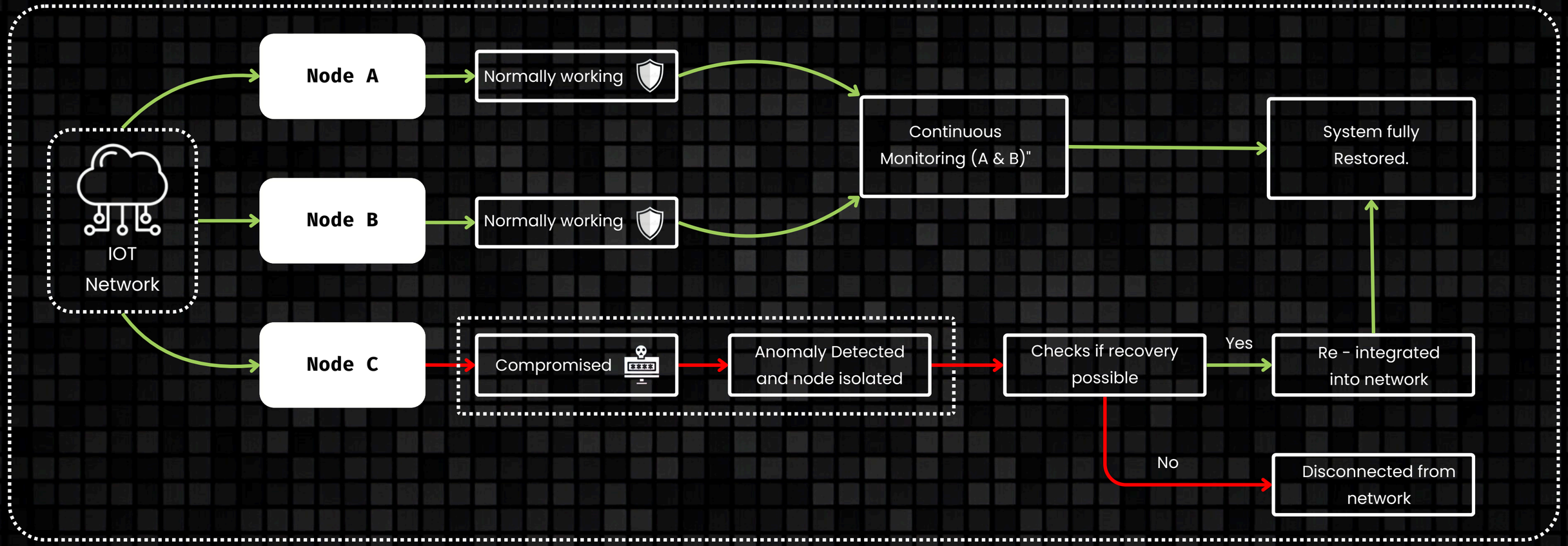
Dashboard Interface

- **Real-Time Node Map**: Visualizes all containerized nodes in the network with their status, highlighting threats and isolated nodes.
- **Node Insights:** Clicking on a node displays metrics like anomaly scores, bytes sent/received, and recovery actions.
- **Anomaly Notifications:** Alerts for detected threats, isolated nodes, and recovery events, ensuring real-time awareness.
- **Audit Logs:** Provides exportable records of isolation/recovery history and flagged MAC addresses for compliance and analysis.



CODE RED '25

PROCESS FLOW



Our system logs all detection, isolation, and recovery actions for auditing. Real-time alerts keep administrators updated on anomalies and recovery, while post-incident analysis and metrics help refine the system for better future responses.

CODE RED '25

TEAM DETAILS

Team Leader Name : Prabu Jayant

Student ID: 1RV22CY044

Phone Number: 8904261616

Email ID: prabujayant.cy22@rvce.edu.in

Member 1 Name : Elvis Vincent

Member 2 Name : Naomi Andrea Pereira

Member 3 Name : Varshith Y

CODE RED '25