GridSAFE: Cyber Simulation of Grid Attacks with AI Anomaly Detection

Team: SMDAY-08
Members: Nellie Leaverton, Jason, Kyle, Evan, Anthony, Brant

Purpose & Context

Cybersecurity Education

GridSAFE provides an engaging platform for students and educators to learn about cybersecurity concepts involving critical infrastructure through a practical simulation.

Infrastructure Security Awareness

The project simulates cyberattacks on power grids to help educations to spread awareness about infrastructure security.
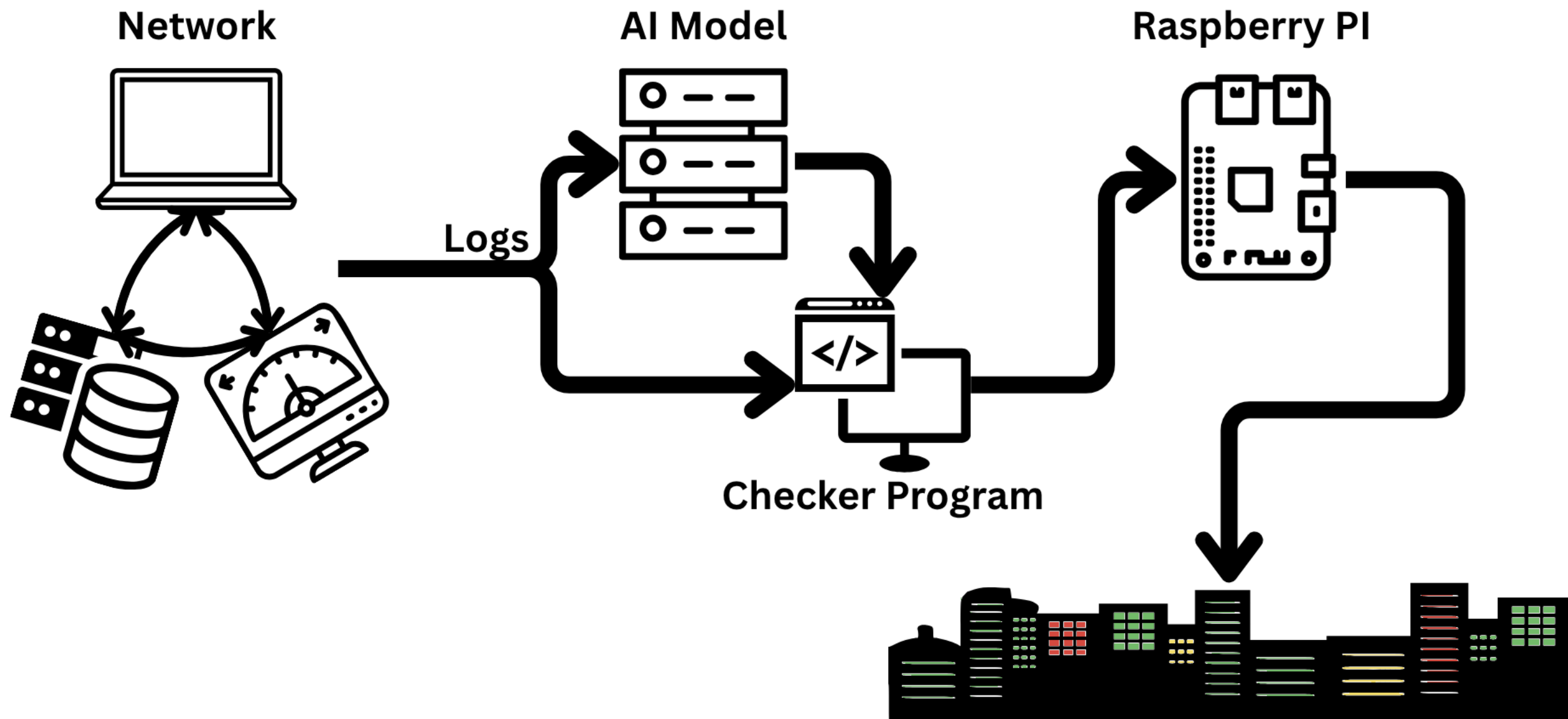
Target Audience

Educators, students, and individuals interested in cybersecurity in critical infrastructure.

Low-Cost Interactive Tool

This accessible, user-friendly platform bridges theory and practical application.

System Architecture

Network

AI Model

Raspberry PI

Logs

Checker Program

Technical Requirements and Progress

Software/Cyber Requirements

Functional Requirements

Full network log analysis with reporting from our ML model covering high-priority MITRE ATT&CK techniques.

Software and Analytics

System logs accurately analyzed with machine learning, with editable configuration and modular design.

- Cover at least 20 attacks

- At least 80% accuracy

Hardware Requirements

Functional Requirements

Real-time data processing with 1-2 second LED control and support for fail-safe and manual overrides.

Physical Design

Compact 3x3 ft city model using non-conductive materials and securely enclosed wiring for safety.

Design Trade-Offs

Balanced Design Trade-offs
- Balances usability, functionality, and cost for effective classroom deployment.

Economic Feasibility
- Uses affordable, open-source, and 3D-printed materials.
- Achieves low-cost implementation compared to proprietary government simulators.

Human-Centered Design
- Promotes hands-on, visual learning experiences.
- Helps students and professionals understand real cyberattack impacts on critical infrastructure.

Technical Integration
- Combines hardware and software components.
- Includes 3D-printed city models, LEDs, Raspberry Pis, and an AI-based IDS.
- Simulates real-world cyberattacks on power grids.

Progress & Reflection (Plus-Delta)

Plus, Delta Progress, Delta Understanding

- Technical (Feasibility)
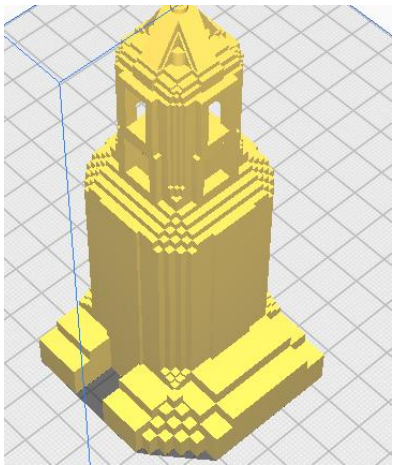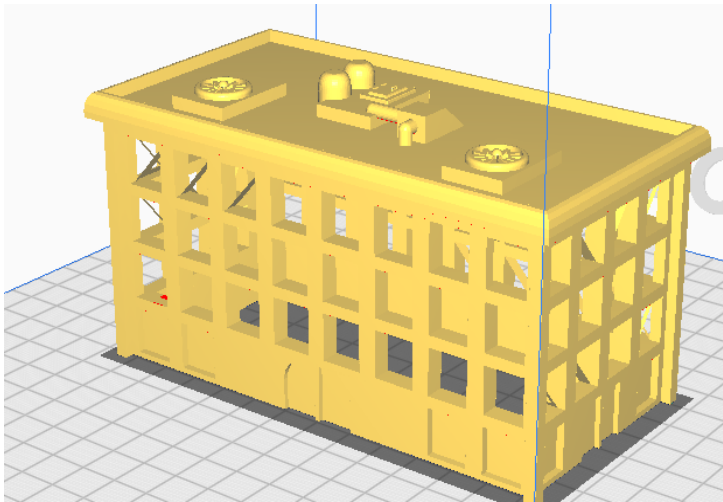- Economic (Viability)
- Human (desirability)

Log Type	timestamp	node_id
Plant	2025-10-02T15:00:01Z	Plant1
	2025-10-02T15:05:22Z	Plant1
Substation	2025-10-02T15:01:45Z	SubstationA
	2025-10-02T15:06:10Z	SubstationA
Smart Meter	2025-10-02T15:02:30Z	Meter12
	2025-10-02T15:07:12Z	Meter12
Baseline Logs	2025-10-02T08:00:00Z	Plant1
	2025-10-02T08:05:00Z	Plant1
	2025-10-02T08:10:00Z	Plant1
	2025-10-02T08:15:00Z	Plant1
	2025-10-02T08:20:00Z	Plant1
	2025-10-02T08:25:00Z	Plant1
	2025-10-02T08:30:00Z	Plant1
	2025-10-02T08:35:00Z	Plant1
	2025-10-02T08:40:00Z	Plant1
	2025-10-02T08:45:00Z	Plant1

THANK YOU
Q & A