Problem statement

As IoT devices proliferate, securing them from evolving cyber threats has become increasingly complex. Traditional security solutions struggle to detect and mitigate real-time attacks, leaving systems vulnerable to breaches and exploitation

Problems with Traditional security methods :

- Inability to Handle Real-Time Threats
- Scalability issues
- Lack of adaptability
- High False Positives/Negatives
- Limited Contextual Understanding

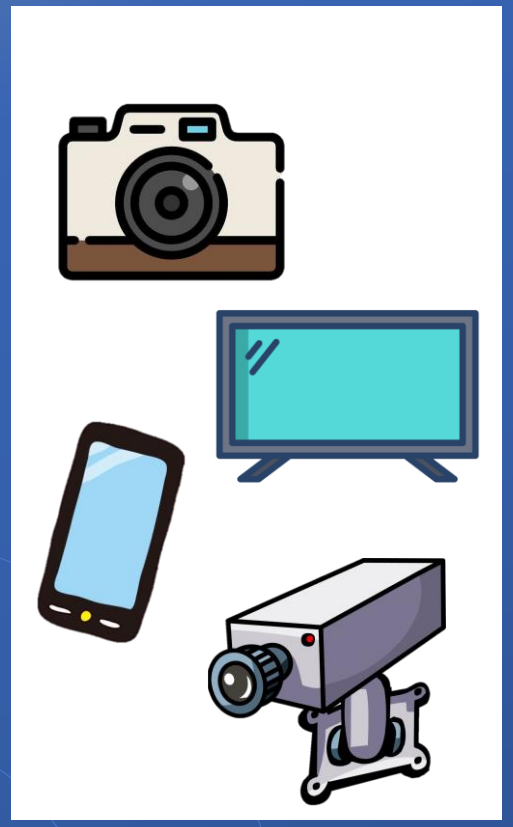
Solution

- Leverage AI/ML to detect unusual behavior and identify emerging threats in real time.
- Automatically set anomalies as top priority and allocate resources to address threats immediately.
- Analyze conditions, time, and patterns of anomalies, enabling the system to adapt and prevent future attacks dynamically.
- Disconnect the compromised IoT device from the network, using a secure proxy to monitor and control its activities until recovery.
- Update AI/ML models with each incident to enhance detection accuracy, minimize false positives/negatives, and future-proof the system.

Architecture

Admin Monitoring Dashboard

IoT devices



IoT Gateway

AI based threat detection

- Isolate compromised device
- Break Connection with IoT Network
- Set Proxy for Affected Devices
- Set Proxy for Affected Devices

Impact

Short term

- Real-Time Threat Detection
- Incident Response
- Faster Reaction Times
- Decreased False Positives

Long term

- Scalability
- Adaptability to New Threats
- Automated Response and Self-Healing
- Proactive Threat Prevention
- Long-Term Cost Savings