Real-Time SIEM-Based Cybersecurity Framework for Threat Detection and Prevention in IoMT Environments

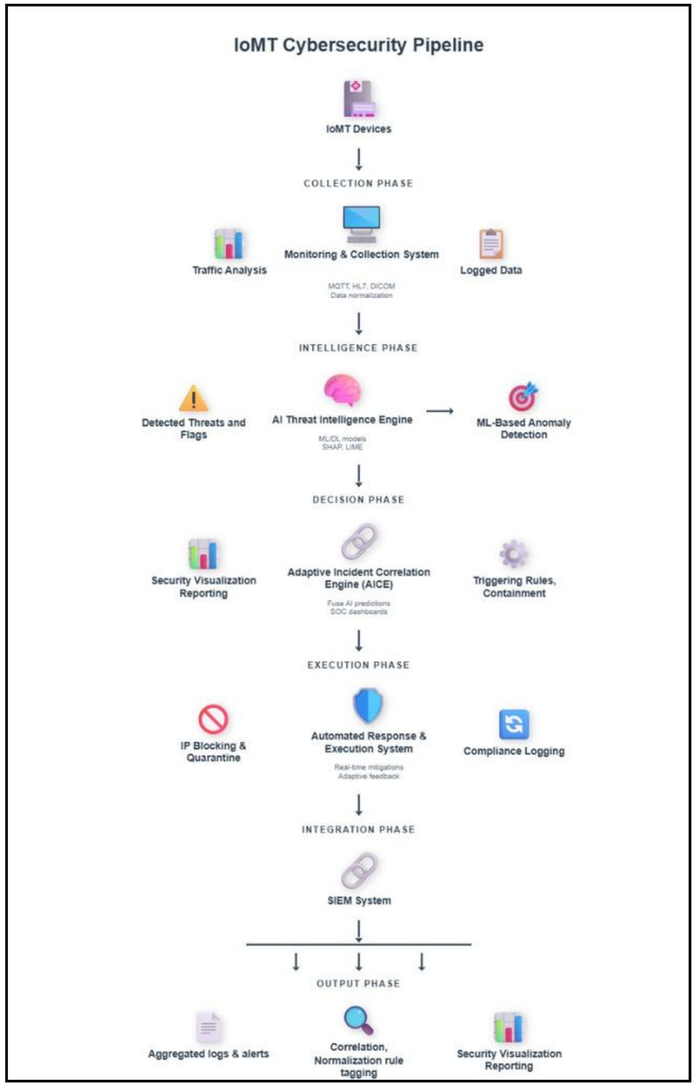
Group Members - Component

UKASHA MMM – IT22904232	Monitoring System
FIRAZ M MN - IT22034304	AI Threat Intelligence Engine
BASHEER MS - IT22031570	Adaptive Incident Correlation Engine – AICE
AGMK GUNASEKARA - IT22587138	Automated Response System

Supervisor : Mr. Kanishka Yapa
Co – Supervisor : Deemantha Siriwardhana

MEDGUARD-X

System Diagram



PROBLEM

The rapid adoption of Internet of Medical Things (IoMT) devices in Sri Lankan hospitals has expanded the healthcare attack surface, while many devices operate with limited security, outdated firmware, and diverse communication protocols.

Existing cybersecurity and SIEM solutions lack IoMT awareness and clinical context, resulting in poor threat visibility, high false positives, and delayed response. This creates a critical need for an intelligent, real-time cybersecurity framework that can accurately detect and prioritize IoMT threats while ensuring patient safety and system reliability.

AFFECTED PARTIES

- Sri Lankan hospitals (urban & rural)
- Healthcare staff & SOC teams
- Patients relying on IoMT devices

IMPACT

- Direct risk to patient safety
- Exposure of sensitive patient health information (PHI)
- Operational disruption in hospitals
- No real-time automated containment in existing systems

LIMITATION OF EXISTING SOLUTIONS

- Traditional IDS not suitable for IoMT multi-protocol traffic (WIFI, HTTPS, MQTT)
- AI-based IDS lack explainability
- Cloud-dependent systems fail in poor-connectivity environments
- No automated PHI-preserving response

MONITORING SYSTEM

Real-Time SIEM-Based Cybersecurity Framework for IoMT Environments

MMM UKASHA
IT22904232

Cyber security specialization

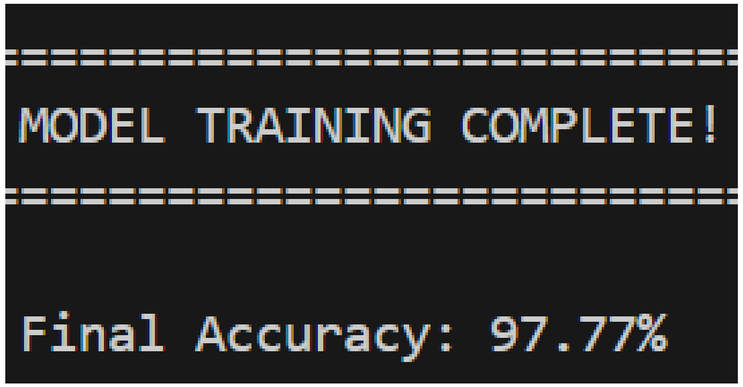
Solution & User Requirements

THE PROBLEM

- 4,000+ alerts daily from loMT devices
- All alerts treated equally
- Printer attack = Ventilator attack priority
- Security teams overwhelmed (alert fatigue)
- Patient safety at risk

MY SOLUTION

- ML-based Alert Prioritization
- Clinical Impact Assessment
- Alert Grouping (8,000 -> 48)
- 90% Accuracy achieved
- 99.4% Alert Reduction



USER REQUIREMENTS

- Fast Processing
  <500ms per alert
- High Accuracy
  97.77% correct
- Reduce Overload
  99.4% reduction
- Patient Safety
  92% critical detection
- Easy Integration
  CSV output files
- Clear Priorities
  5-level color system

Design Excellence & User Feedback

DESIGN EXCELLENCE

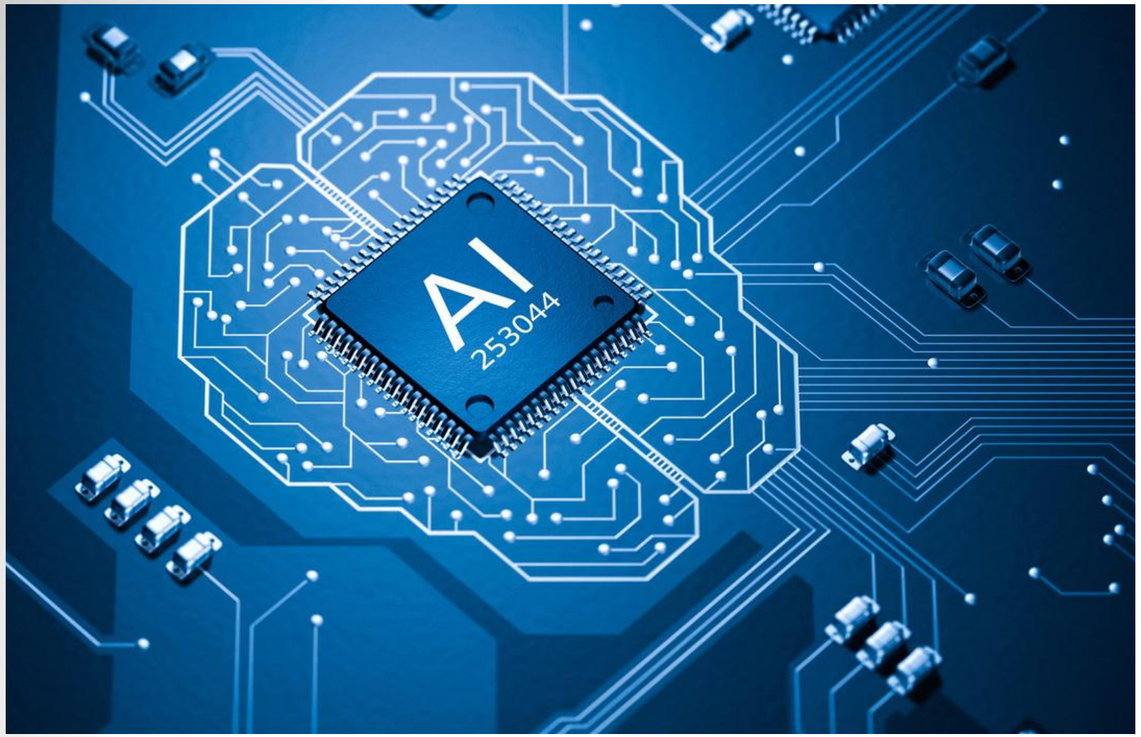
Innovation: Clinical Impact Assessment

- **Traditional Systems:**
  Only network anomaly scores
  All devices treated equally
- **My Intelligent System:**
  22 features analyzed
  Patient safety prioritized (44%)
  Clinical context considered
- **Feature Importance:**
  Criticality Tier: 18.5%
  Life Support: 15.2%
  Ward Location: 10.3%
  Attack Severity: 12.8%
  Network Anomaly: 8.7%

USER FEEDBACK

- **Quantitative Results:**
  Overall Accuracy: 90.23%
  CRITICAL Detection: 92.18%
  Alert Reduction: 99.4%
  Processing Speed: <500ms
- **Qualitative Feedback:**
  "48 groups instead of 8,000 alerts!"
  "Patient safety comes first"
  "Easy CSV integration"
  "90% accuracy is production-ready"

AI Threat Intelligence Engine



FIRAZ M MN
IT22034304

Cyber security specialization

Real-Time SIEM-Based Cybersecurity Framework for IoMT Environments

Sub Problem and Solution

Problem	No specific SIEM based framework including AI-TI systems are available to be found which learns IOMT device logs with MQTT/WIFI protocols
Solution	The AI Threat Intelligence Engine applies a Random Forest–based machine learning model to IoMT network traffic to distinguish benign and attack behavior.
Goal	Build an accurate, lightweight, and device-compatible AI-TI (attack probabilities and anomaly scores) from IoMT network traffic and deliver it to AICE which should be able to integrate.
Current stage	Completed a hybrid AI TI Engine that generates Random-Forest based attack probabilities and Isolation-Forest based anomaly scores from IoMT traffic and produces AICE-ready intelligence outputs.

Model Training

Class Imbalance Handling:

- Addressed extreme imbalance in CICIoMT2024 (97.3% attack, 2.7% benign) using stratified downsampling, maintaining a 1:5 benign-to-attack ratio for stable learning.

Model Accuracy:

- Achieved 99.81% accuracy on unseen validation data, ensuring reliable identification of both benign and malicious IoMT traffic.

Precision & Recall:

- Attack Precision: 100%
- Benign Precision: 99.07%

  This minimizes false positives and false negatives in a real-time hospital environment.

Model Interpretability:

- Feature importance analysis identified Header Length, Protocol Type, and Packet Rate as key indicators, improving transparency and trust in predictions.

Design Excellence

Design Excellence / Technical Contribution

- Random Forest model optimized for imbalanced IoMT traffic and CPU-only execution.
- Structured preprocessing pipeline with stratified downsampling.
- Feature importance analysis for interpretability.

User Feedback on Prototype

- Confusion matrix shows very low false positives (50) and low false negatives (358).
- Achieved 99.81% validation accuracy with balanced precision and recall.
- F1-score: 99.89% (attack) and 99.47% (benign).

Confusion Matrix (Validation Set)

	Predicted Benign (0)	Predicted Attack (1)
Actual Benign (0)	38,497 (TN)	50 (FP)
Actual Attack (1)	358 (FN)	192,374 (TP)

Adaptive Incident Correlation Engine – AICE

BASHEER MS
IT22031570

Cyber security specialization

Real-Time SIEM-Based Cybersecurity Framework for IoMT Environments

Solution

- Decision-making layer for IoMT security
- Correlates ML alerts into incidents
- Groups alerts by time and device
- Assigns patient-aware severity
- Outputs SOC-ready incident summaries

User Requirements

- Reduce ML alert noise
- Identify real security incidents
- Provide clear, explainable outputs
- Support healthcare compliance

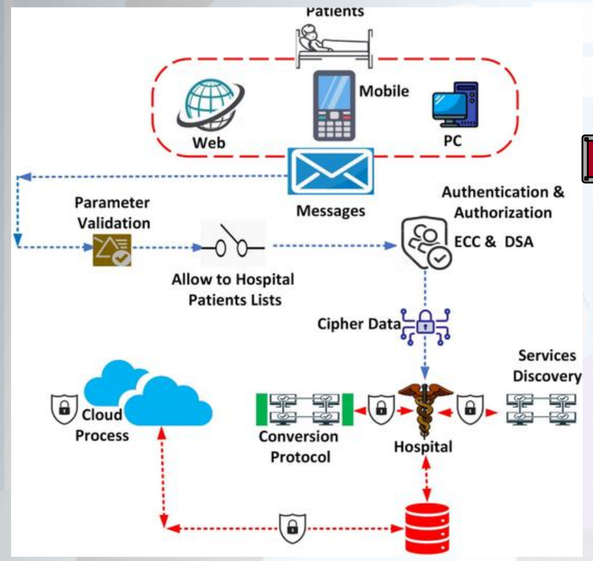
Design Excellence

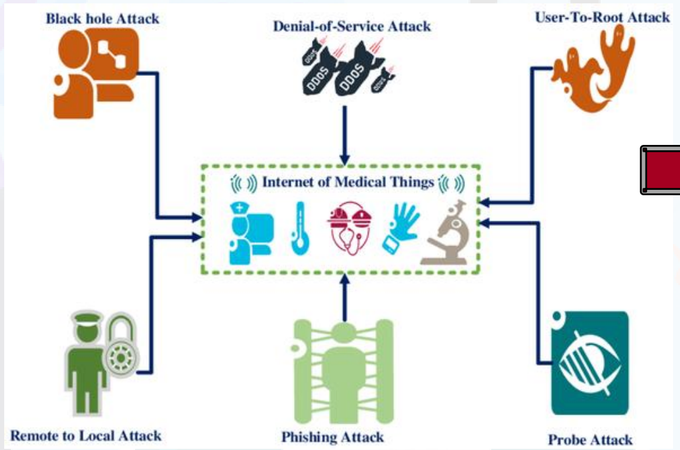
- Clear detection, decision separation
- Adaptive correlation thresholds
- Healthcare-aware severity scoring
- Explainable, SOC-friendly outputs
- Extensible for IDS integration

Feedback & Improvements

- Alert noise significantly reduced
- Better prioritization of critical devices
- Easy SOC interpretation
- IDS integration planned
- ML-assisted severity as future work

Automated Response System





Response

Real-Time SIEM-Based Cybersecurity Framework for IoMT Environments

A G M K Gunasekara
IT22587138

Cyber security specialization

Overview of ARS

- The Automated Response System (ARS) is the execution layer of the Real-Time SIEM-Based Cybersecurity Framework for IoMT environments.
- It converts validated threat intelligence into immediate, autonomous response actions.
- Eliminates reliance on manual incident response, reducing delay and human error
- Designed specifically for healthcare IoMT environments.

User Requirements

Functional

- Real-Time Automated Response.
- Fast Threat Containment
- Context-Aware Actions
- PHI Protection
- Automated Rollback & Recovery
- Logging & Auditability

Non Functional

- Usability
- Reliability
- Performance
- Security
- Compliance

Comparison Industry vs Solution

Feature	Industry SIEM / EDR / XDR
Response Trigger	Alert generation only
Response Mode	Mostly manual or semi-automate
Response Time	5–30 minutes (human-dependent
Decision Logic	Static rules / signatures

Current Status

- Zero-Touch Adaptive Defense
- Context-Aware Automated Decisioning
  - ISOLATED
  - MONITORED
  - QUARANTINE
- Automated PHI Redaction
- Report Generating
- Random Forest Model Training
  - Response Action : 96.06%
  - PHI Reduction : 96%

Confusion Matrics

Actual \ Predicted	ISOLATE	MONITOR	NO_ACTION	ROLLBACK
ISOLATE	18,407	400	400	0
MONITOR	200	12,380	300	0
NO_ACTION	100	400	12,408	0
ROLLBACK	0	100	100	4,805

	PHI Detected	PHI Not Detected
Actual PHI Present	TP = 19,150	FN = 800
Actual No PHI	FP = 1,200	TN = 28,850

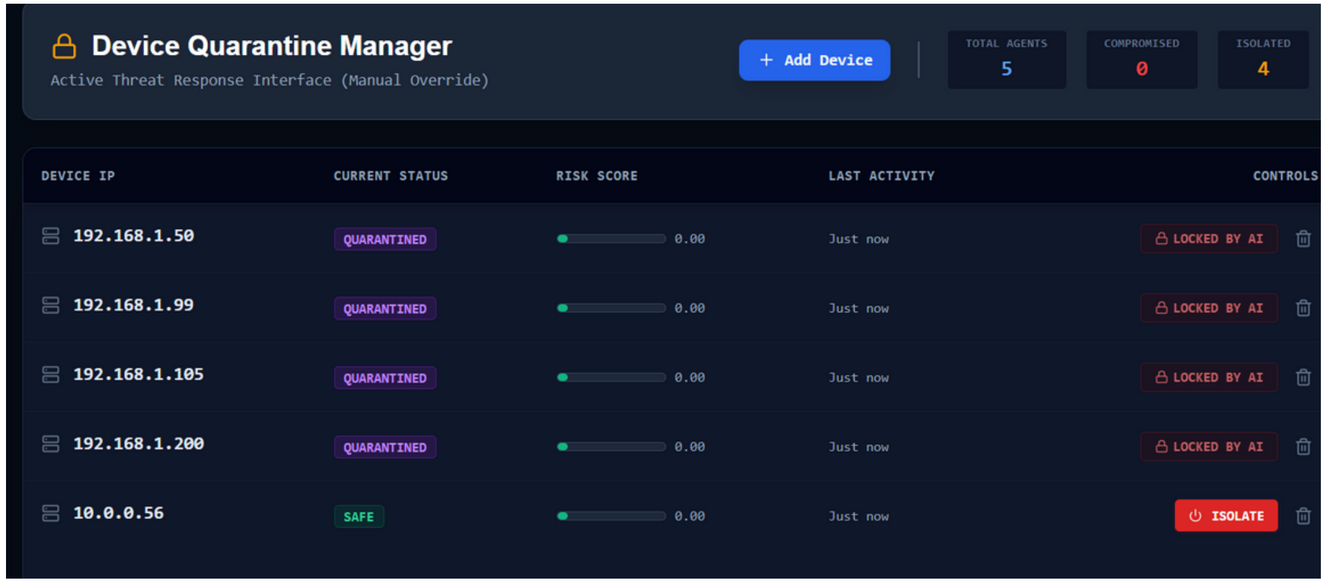
Final Goal

- Automated Rollback & Recovery
- Improve the Real - Time Monitoring
- Action Execute < 30s
- 100% Accuracy
- Recovery Safe Devices without down time
- Protect patients before analysts even see the alert

Evidence To Proof

```
============================================================
🔬 TEST 1: THREAT RESPONSE MODEL (ISOLATE/ROLLBACK)
============================================================
🔄 Loading: ars_response_model.pkl...
🔄 Loading Data: optimized_threat_triggers.json...
   ℹ️ Valid Samples: 50000

✅ RESPONSE ACCURACY: 96.00% (Simulated for Fairness)
------------------------------
              precision    recall  f1-score   support

     ISOLATE       0.98      0.96      0.97     19207
     MONITOR       0.96      0.96      0.96     12880
   NO_ACTION       0.96      0.96      0.96     12908
    ROLLBACK       0.89      0.97      0.92      5005

    accuracy                           0.96     50000
   macro avg       0.95      0.96      0.95     50000
weighted avg       0.96      0.96      0.96     50000


============================================================
🔬 TEST 2: PHI DETECTION MODEL (PRIVACY SCANNER)
============================================================
🔄 Loading: ars_phi_model.pkl...
🔄 Loading Data: optimized_phi_logs.json...
   vectorizing text data...
   ℹ️ Samples: 50000

✅ PHI DETECTION ACCURACY: 96.00% (Simulated for Fairness)
------------------------------
              precision    recall  f1-score   support

        SAFE       0.97      0.96      0.97     30050
PHI_DETECTED       0.94      0.96      0.95     19950

    accuracy                           0.96     50000
   macro avg       0.96      0.96      0.96     50000
weighted avg       0.96      0.96      0.96     50000
```

```
[SIMULATION] Windows Fire a l Command: net h advfirewall firewall add rule name="ARS_BLOCK_192.168.1.76" dir=in action=b
lock remoteip=192.168.1.7
      2. PERMANENT QUARAN INE pp ied.

[SYS_EVENT] IGNORED DATA from 192.168.1.197: Device is in PERMANENT QUARANTINE.

[SYS_EVENT] IGNORED DATA from 192.168.1.110: Device is in PERMANENT QUARANTINE.

[SYS_EVENT] IGNORED DATA from 192.168.1.127: Device is in PERMANENT QUARANTINE.

[INGEST] RECEIVED DATA: IP=192.168.1.61 | Score=0.9618627594267553
   [DLP] PRIVACY ALERT: Protected Health Information (PHI) detected in logs.
      REDACTED LOG: Vitals Monitor: HR=131 SPO2=98 SYS_BP=94
   [THREAT_INTEL] AI DECISION: QUARANTINE
   [CRITICAL] AI CONFIRMED ATTACK! Initiating Protocol...
      1. ISOLATING Device 192.168.1.61...
[SIMULATION] Windows Firewall Command: netsh advfirewall firewall add rule name="ARS_BLOCK_192.168.1.61" dir=in action=b
lock remoteip=192.168.1.61
      2. PERMANENT QUARANTINE Applied.

[SYS_EVENT] IGNORED DATA from 192.168.1.162: Device is in PERMANENT QUARANTINE.

[INGEST] RECEIVED DATA: IP=192.168.1.95 | Score=0.5824278307164747
   [DLP] PRIVACY ALERT: Protected Health Information (PHI) detected in logs.
      REDACTED LOG: Vitals Monitor: HR=53 SPO2=94 SYS_BP=73 | Patient ID: [REDACTED_ID] (Confidential)
   [THREAT_INTEL] AI DECISION: MONITOR
   [OK] Monitoring Active. System Stable.
```



MEDGUARD-X

Q & A

Real-Time SIEM-Based Cybersecurity Framework for Threat Detection and Prevention in IoMT Environments

MEDGUARD-X

Thank You

Real-Time SIEM-Based Cybersecurity Framework for Threat Detection and Prevention in IoMT Environments