HOME

MEDGUARD-X

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

SLIIT FACULTY OF COMPUTING

25-26J-70

Cyber Security

2026 - 03 - 09

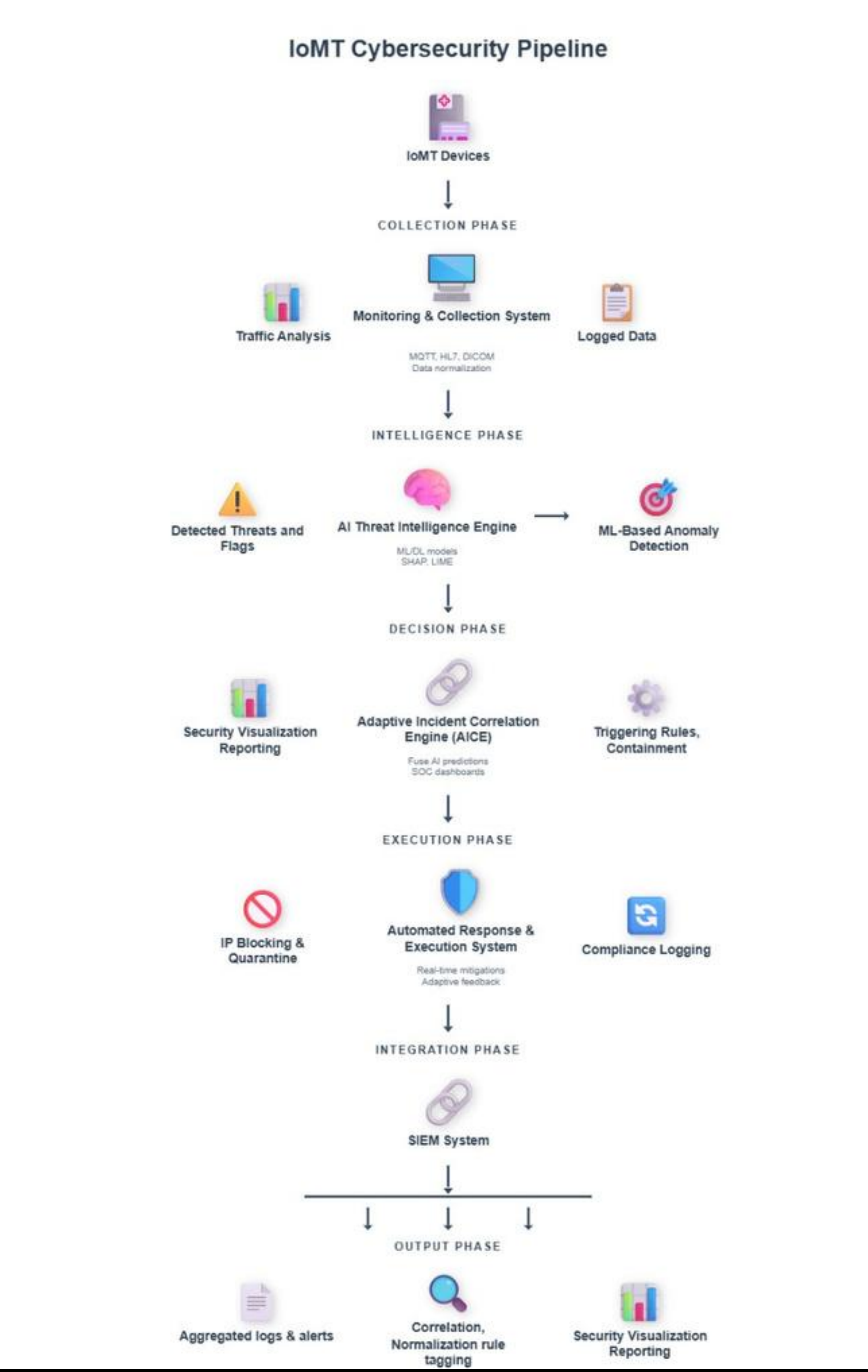
Group Members - Component

Member	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



MEDGUARD-X

CONTEXT

Modern hospitals use **IoMT (Internet of Medical Things) devices** such as:

- ECG Monitors
- Pulse Sensors
- Temperature Sensors
- Patient Monitoring Systems

PROBLEM

- IoMT networks are vulnerable to cyber attacks , DoS attacks, Malware attacks, Unauthorized access.

MEDGUARD-X

GAP AND MAIN OBJECTIVE

Main Objective

Develop a **real-time IoMT-aware SIEM framework** that detects cyber threats, reduces alert overload, and prioritizes incidents based on patient safety.

Research GAP

- ❑ **Existing SIEM systems lack IoMT awareness**
- ❑ **No clinical impact–based alert prioritization**
- ❑ **High alert volume causes SOC overload**
- ❑ **No automated response for IoMT threats**

MEDGUARD-X

Solution Overview

A **lightweight AI-powered SIEM-based cybersecurity framework** designed for IoMT hospital environments that detects anomalous device behavior, correlates alerts, and supports automated response to protect patient safety and medical data.

Key Features Delivered

- ❑ AI Threat Detection Engine
  Analyzes IoMT network traffic and device logs using machine learning models (Random Forest and Isolation Forest) to detect anomalies and generate threat intelligence.
- ❑ Intelligent Monitoring & Alert Prioritization
  Processes IoMT alerts, groups related events, and prioritizes incidents based on device criticality and patient safety impact.
- ❑ Adaptive Incident Correlation & Automated Response
  Correlates alerts from AI models and IDS logs to generate actionable incidents and supports automated containment such as device isolation and recovery.

Current Completion Status

Overall Completion – 80%

- ❑ IoMT hospital environment simulation created using ESP devices and sensors.
- ❑ Device logs successfully collected and stored in the database.
- ❑ Individual machine learning models trained and validated.
- ❑ System integration between components (Monitoring, AI Engine, AICE, Response) is currently in progress.
- ❑ Real-time response execution and full SIEM pipeline integration remain pending.

System Architecture

Components

Component A – Monitoring System
Owner: IT22904232 – MMM Ukasha
Responsible for collecting IoMT device logs, monitoring network traffic, and generating prioritized alerts using machine learning–based alert management.

Component B – AI Threat Intelligence Engine
Owner: IT22034304 – Firaz M MN
Processes IoMT network traffic and device logs using machine learning models (Random Forest, Isolation Forest) to detect anomalies and generate attack probability scores.
Component C – Adaptive Incident Correlation Engine (AICE)

Owner: IT22031570 – Basheer MS
Correlates alerts from AI models and IDS systems, assigns severity levels based on device criticality and patient safety, and generates SOC-ready incident summaries.

Component D – Automated Response System (ARS)
Owner: IT22587138 – A.G.M.K Gunasekara
Executes automated containment actions such as device isolation, PHI redaction, and rollback recovery to protect hospital systems.

Integration Points (APIs / Data Formats)

- WebSocket communication for real-time device data streaming
- MQTT protocol for IoMT device communication
- WiFi traffic analysis from ESP-based IoMT devices
- Data exchange formats: CSV and JSON
- MongoDB database used for storing logs, alerts, and device data
- Pipeline architecture connecting monitoring → AI detection → correlation → response system

Deployment / Runtime Setup

- **IoMT Device Layer:** ESP controllers and sensors generating device data
- **Network Layer:** WiFi-based communication with MQTT and WebSocket protocols
- **Processing Layer:** AI models and correlation engines running on a central machine/server
- **Database Layer:** MongoDB for log storage and event tracking
- **System Architecture:** Full pipeline integration connecting all components for real-time threat detection and response

Faced Challenges

MEDGUARD-X

System Integration Challenges

Initial architecture planned CSV-based data sharing between components, but this approach is not suitable for real-time processing.

To achieve real-time detection and response, the system must be redesigned using a continuous data pipeline architecture.

IoMT Device Development Challenges

Building ESP-based IoMT devices and sensors for testing the hospital environment required significant hardware configuration.

Generating realistic device logs from medical sensors is complex and time-consuming.

Data Collection & Communication Challenges

Device logs must be collected directly through APIs or endpoints rather than static files.

Implemented MQTT broker communication to stream device data and store it in the MongoDB database.

Component Integration Issues

Components are currently working independently, but full pipeline integration is still under development.

Because of this, the Automated Response System cannot yet trigger real device actions.

Network & Performance Constraints

All IoMT devices must operate within the same local network, which limits scalability.

Processing latency increases due to centralized data processing and multiple system components.

Data Consistency Challenges

Data is received from multiple endpoints and protocols, causing difficulties in:

- Data synchronization
- Format standardization
- Real-time processing

Commercialization & Real-World Use

Target Users / Market

- ❑ Sri Lankan hospitals (public and private) using IoMT medical devices
- ❑ Healthcare IT departments and SOC teams responsible for cybersecurity monitoring
- ❑ Clinical engineers managing connected medical equipment
- ❑ Future expansion to South Asian healthcare systems with similar infrastructure constraints

Cost and Feasibility

- ❑ Uses **open-source technologies** (Python, ML frameworks)
- ❑ Estimated **development and deployment cost:**
  Initial prototype: **50,000 – 70,000 LKR**
  Infrastructure: existing hospital servers or cloud deployment
- ❑ Low hardware requirements allow deployment on **standard hospital IT infrastructure**

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