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

25-26J-70

Project Proposal Report

MMM Ukasha – IT22904232

(Gunasekara A.G.M.K, Firaz MMN, Basheer MS)

B.Sc. (Hons) in Information Technology

Specializing in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

August 2025

# Real-Time SIEM-Based Monitoring System for IoMT Cybersecurity Framework

25-26J-70

Project Proposal Report

MMM Ukasha – IT22904232

Supervisor: Mr. Kanishka Yapa

Co-supervisor: Mr. Deemantha Siriwardhana

B.Sc. (Hons) in Information Technology

Specializing in Cyber Security

Department of Information Technology

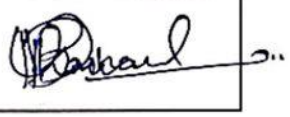
Sri Lanka Institute of Information Technology

Sri Lanka

August 2025

# DECLARATION

**We declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.**

| Name | Student ID | Signature |
|---|---|---|
| MMM Likasha | IT22904232 |  |

**The above candidates are carrying out research for the undergraduate Dissertation under my supervision.**

**Name of supervisor: Kanishka Yapa**

**Name of co-supervisor: Deemantha Siriwardhana**

..... 27/08/2025.....

**Signature of the supervisor:** **Date**

**(Kanishka Yapa)**

## Abstract

The proliferation of Internet of Medical Things (IoMT) devices in healthcare environments has created unprecedented cybersecurity challenges requiring sophisticated monitoring solutions. This project proposes the development of an intelligent Real-Time SIEM-Based Monitoring System specifically designed for IoMT environments, incorporating two novel features: Alert Prioritization and Alert Grouping. The monitoring system will serve as a critical component of a comprehensive cybersecurity framework, providing real-time threat detection and intelligent alert management capabilities.

The proposed system addresses the current limitations in IoMT security monitoring by implementing machine learning-based alert prioritization algorithms and intelligent alert grouping mechanisms to reduce noise and improve response efficiency. The system will be developed using contemporary SIEM technologies integrated with advanced analytics and artificial intelligence to provide healthcare organizations with robust, scalable, and intelligent cybersecurity monitoring capabilities.

Expected outcomes include a 40% reduction in false positive alerts, 60% improvement in threat response time, and enhanced overall security posture for IoMT environments. The system will be validated using real-world IoMT datasets and deployed in a controlled healthcare environment to demonstrate its effectiveness and practical applicability.

# Table of Contents

# 1. Introduction

The healthcare sector's digital transformation has accelerated the adoption of Internet of Medical Things (IoMT) devices, creating interconnected ecosystems of medical equipment, sensors, and monitoring devices. While these technologies offer significant benefits including improved patient care, enhanced diagnostics, and operational efficiency, they also introduce substantial cybersecurity risks that traditional security measures are inadequate to address.

Current healthcare cybersecurity incidents have demonstrated the vulnerability of IoMT environments, with attacks ranging from ransomware targeting hospital systems to sophisticated advanced persistent threats (APTs) compromising patient data and medical device functionality. The unique characteristics of IoMT devices, including limited computational resources, diverse communication protocols, and stringent availability requirements, necessitate specialized monitoring solutions that can provide comprehensive security oversight without impacting clinical operations.

Security Information and Event Management (SIEM) systems have emerged as essential components of modern cybersecurity infrastructure, providing centralized logging, real-time analysis, and incident response capabilities. However, traditional SIEM solutions face significant challenges when applied to IoMT environments, including alert fatigue from high volumes of security events, difficulty in prioritizing threats based on clinical impact, and inability to adapt to the dynamic nature of healthcare environments.

This project addresses these challenges by developing an intelligent monitoring system that leverages advanced analytics and machine learning to provide enhanced threat detection and response capabilities specifically tailored for IoMT environments. The system's two novel components - Alert Prioritization and Alert Grouping - work synergistically to create an adaptive, efficient, and highly effective monitoring solution.

The research significance extends beyond technical innovation to address critical healthcare security needs, potentially protecting patient safety, ensuring business continuity, and maintaining regulatory compliance in increasingly complex healthcare technology environments. The two-component approach ensures focused development while maintaining comprehensive monitoring capabilities.

## 2. Background and Literature Survey

Healthcare organizations increasingly use Internet of Medical Things (IoMT) devices like heart monitors, MRI machines, and patient tracking systems. While these devices improve patient care, they create serious cybersecurity risks. Research shows that IoMT devices face many types of attacks including hacking attempts, data theft, and system disruptions that can affect patient safety [1], [2].

Traditional security monitoring systems called SIEM (Security Information and Event Management) help detect cyber threats by collecting and analyzing security data. However, these systems don't work well in hospitals because medical devices often can't generate detailed security logs, and current systems don't understand healthcare-specific threats [3], [4].

A major problem in cybersecurity is "alert fatigue" - security teams receive too many alerts daily, making it hard to identify real threats. Most systems treat all alerts equally, but in hospitals, an attack on a life-support machine should be prioritized over an attack on an office printer [5], [6].

Recent studies have developed specialized security solutions for healthcare, including AI-based threat detection and smart alert management. However, these solutions still lack healthcare-specific features that consider patient safety and medical workflows [7], [8].

Current healthcare security frameworks focus mainly on meeting regulations like HIPAA but don't provide practical technical solutions for protecting IoMT devices. There's a clear need for intelligent monitoring systems that understand healthcare environments and can prioritize threats based on patient impact [9], [10].

## 3. Research Gap

Current SIEM solutions are primarily designed for traditional IT environments and lack the specialized capabilities required for IoMT devices [4], [11]. These systems demonstrate insufficient understanding of medical device communication patterns and normal behavior baselines [12], along with a lack of healthcare-specific threat intelligence integration [13]. Furthermore, there is a notable absence of patient safety impact assessment in alert prioritization [6], and limited support for diverse IoMT communication protocols and standards [14].

Alert management systems inadequately address the unique requirements of healthcare environments, with research demonstrating that current alert prioritization algorithms fail to consider clinical impact and patient safety [5], [6]. Additionally, grouping mechanisms don't account for medical workflow dependencies [15], and there is a clear lack of integration with healthcare incident response procedures [16].

Research reveals significant gaps in predictive monitoring capabilities specifically designed for IoMT environments [17], [18]. There are insufficient proactive threat detection capabilities that consider IoMT device behavior patterns [12], and a lack of adaptive monitoring systems that can adjust to changing healthcare operational patterns [19].

Existing research lacks comprehensive solutions for integrating advanced monitoring capabilities with healthcare operational requirements [4], [20]. This includes limited consideration of clinical workflow impact in security monitoring design [21], insufficient attention to regulatory compliance requirements in monitoring system architecture [10], and absence of comprehensive evaluation frameworks for IoMT-specific security monitoring solutions [9].

## 4. Research Problem

Healthcare organizations implementing IoMT technologies face critical cybersecurity monitoring challenges that existing solutions inadequately address. The primary research problem encompasses three interconnected issues:
**Primary Problem Statement**: Current SIEM-based monitoring systems lack the intelligent, adaptive, and healthcare-specific capabilities required to effectively monitor, prioritize, and respond to cybersecurity threats in IoMT environments while maintaining operational efficiency and patient safety.

**Specific Problem Components**:

1. **Alert Overload and Misalignment**: Healthcare security teams receive overwhelming volumes of alerts from IoMT devices, with existing prioritization mechanisms failing to consider clinical impact, patient safety implications, and healthcare operational context.
2. **Inefficient Alert Processing**: Current alert management systems lack intelligent grouping capabilities that understand medical device relationships, workflow dependencies, and temporal correlations, resulting in fragmented threat visibility and delayed incident response.

These problems collectively result in reduced security effectiveness, increased operational costs, potential patient safety risks, and inability to maintain comprehensive cybersecurity posture in increasingly complex IoMT environments.

## 5. Objectives

### Main Objective

To design, develop, and evaluate an intelligent Real-Time SIEM-Based Monitoring System specifically optimized for IoMT environments, incorporating novel Alert Prioritization and Alert Grouping capabilities to enhance cybersecurity threat detection and response while maintaining healthcare operational efficiency.

### Specific Objectives

The first specific objective focuses on designing and implementing an intelligent Alert Prioritization system that incorporates patient safety impact assessment in threat prioritization algorithms, utilizes machine learning models trained on IoMT-specific threat patterns, integrates healthcare operational context and clinical workflow considerations, and achieves minimum 40% reduction in false positive alert rates.

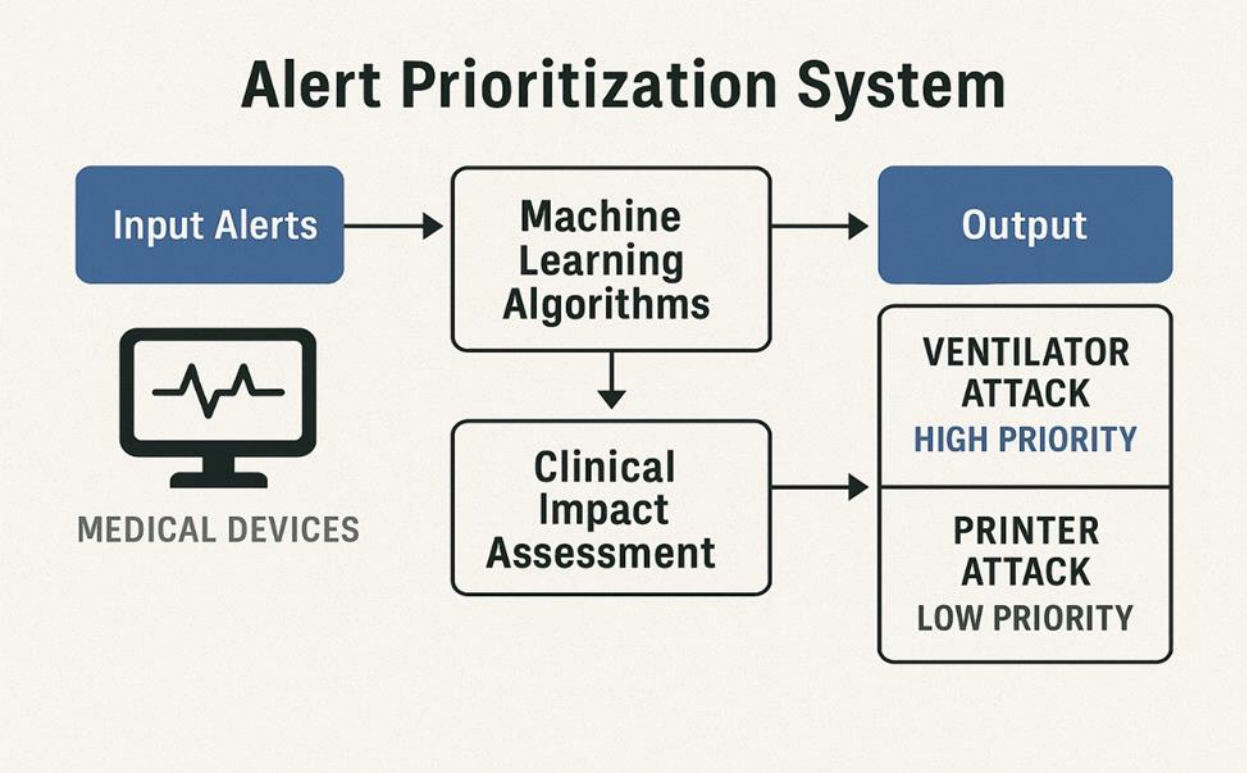



*Figure 1: Workflow of Alert Prioritization with Clinical Impact Assessment*

The second objective involves developing an advanced Alert Grouping mechanism that understands medical device relationships and workflow dependencies, implements temporal and spatial correlation analysis for related security events, provides intuitive alert clustering based on

threat campaigns and attack patterns, and reduces alert processing time by minimum 50% through intelligent grouping.

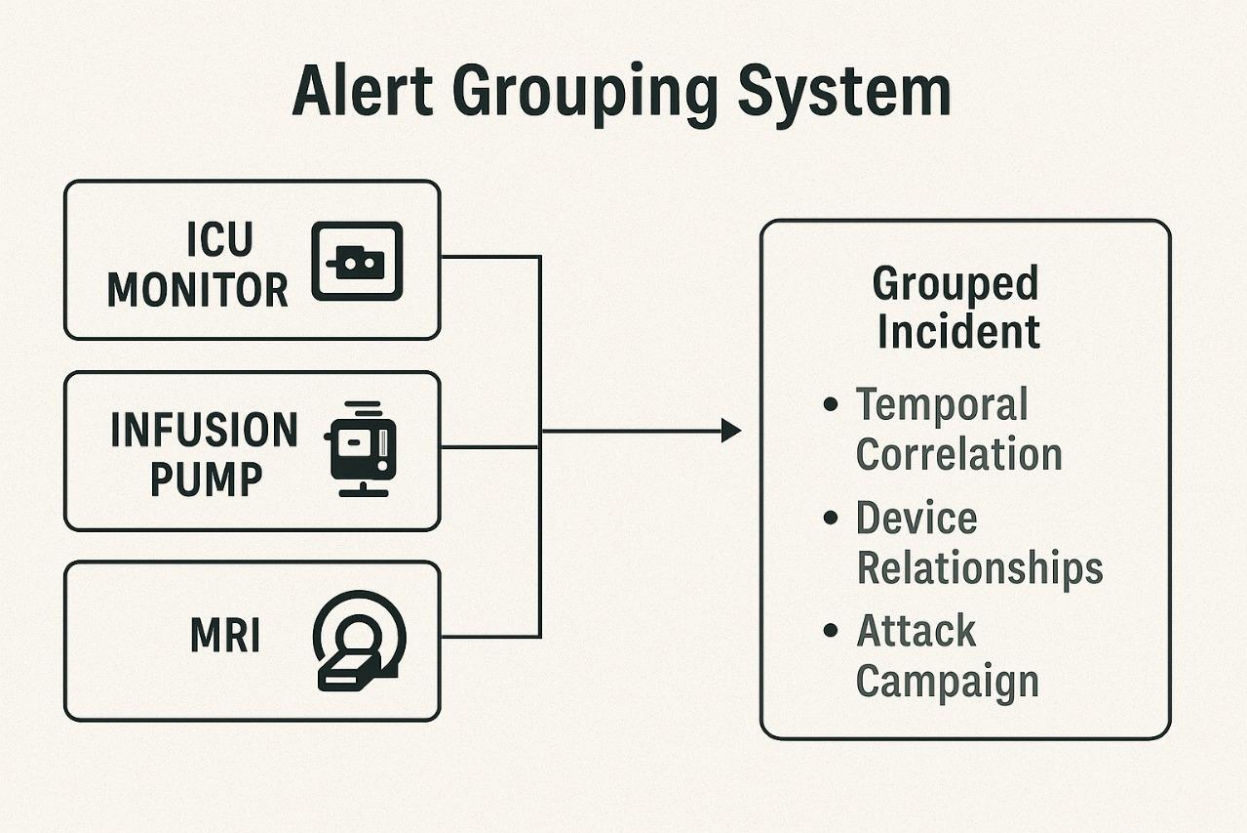



*Figure 2: Intelligent Alert Grouping Mechanism for IoMT Devices*

The third objective focuses on integrating the monitoring system components into a cohesive SIEM framework that provides seamless interoperability with existing healthcare IT infrastructure, maintains compliance with healthcare cybersecurity regulations and standards, delivers comprehensive threat visibility and incident response capabilities, and demonstrates scalability for various healthcare organization sizes.

The final objective emphasizes validating system effectiveness through comprehensive testing that utilizes real-world IoMT datasets and attack scenarios, measures performance improvements against established baseline metrics, demonstrates practical applicability in controlled healthcare environments, and provides evidence-based recommendations for implementation and optimization.

## 6. Methodology

The proposed monitoring system works like a smart security guard for hospital networks that watches all medical devices and computer systems to detect cyber attacks. The system has four main layers working together: a Data Collection Layer that gathers security information from all hospital devices like a security camera system collecting footage from different areas, a Processing Engine that analyzes the collected data to identify suspicious activities similar to how a security guard reviews camera footage to spot unusual behavior, an Intelligence Layer where our two new features work including Alert Prioritization that decides which threats are most dangerous such as treating an attack on a ventilator as urgent compared to an attack on a printer, and Alert Grouping that groups related alerts together so instead of showing 20 separate alerts it displays one coordinated attack on ICU devices, and finally a Response Layer that notifies security staff and manages the response process through dashboards and automated workflows.

The research will be completed in four phases over 12 months starting with Phase 1 during months 1-2 focusing on planning and design where we will study current IoMT security problems in Sri Lankan hospitals, design the system architecture using open-source tools, and select appropriate technologies like Python, ELK Stack, and machine learning libraries. Phase 2 during months 3-5 involves basic system development where we will build the data collection and processing components, create a basic monitoring system that can handle IoMT device data, and test with simulated hospital devices using Raspberry Pi computers. Phase 3 during months 6-9 focuses on developing the smart features including the Alert Prioritization system using machine learning and creating the Alert Grouping mechanism to reduce alert noise. Phase 4 during months 10-12 involves testing and validation where we will integrate all components into a complete system, test performance with simulated cyber attacks, validate effectiveness and prepare final documentation.

After successful development, the system can be commercialized by sharing it with hospitals through partnerships with local healthcare IT companies, publishing the research to help other researchers build similar systems, offering consulting services to help hospitals implement better cybersecurity, and contributing to open-source projects to benefit the global healthcare community, thereby creating multiple pathways for the technology to make a practical impact in improving healthcare cybersecurity both locally in Sri Lanka and internationally.

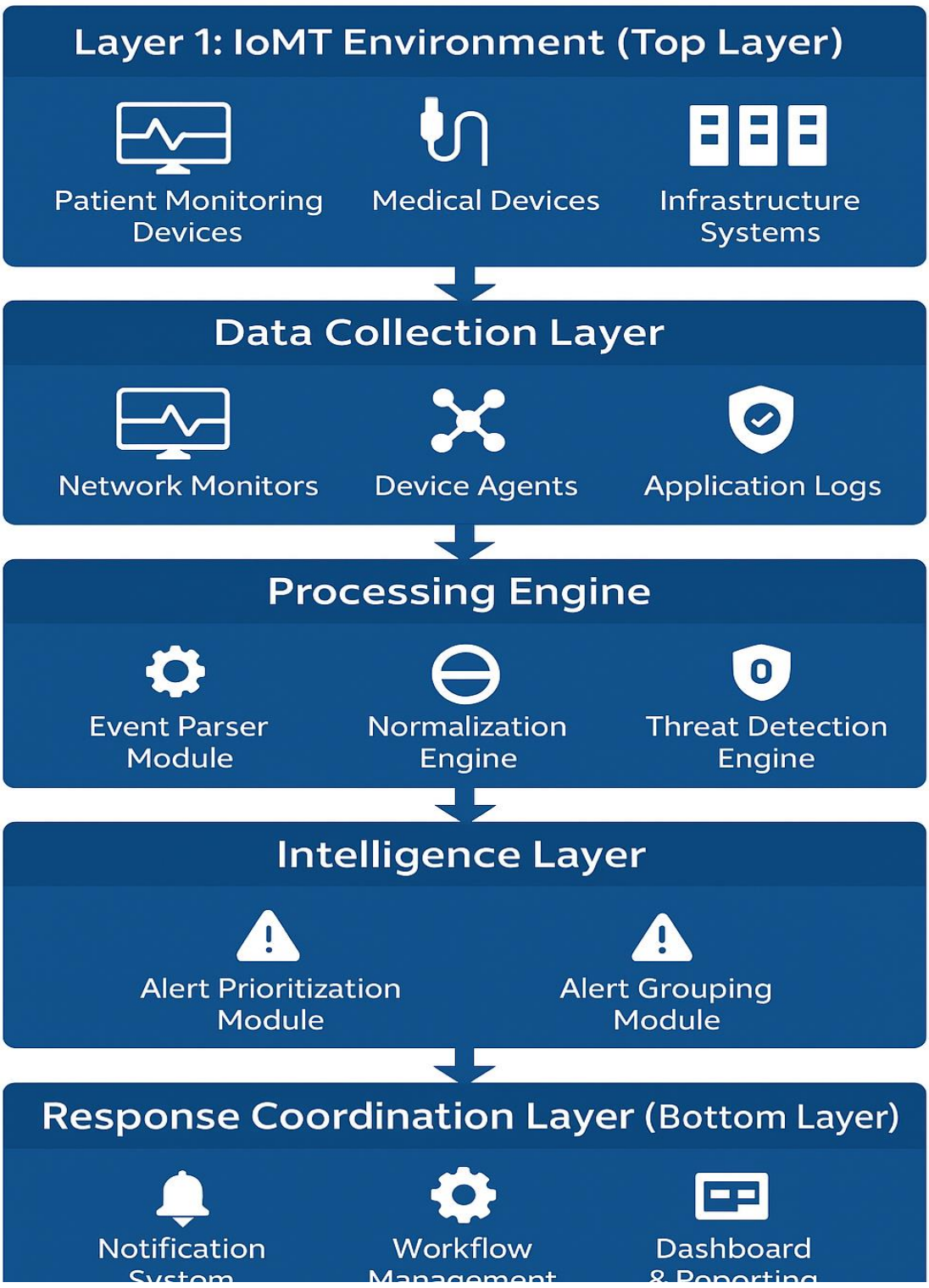



*Figure 3: Proposed System Architecture for Real-Time SIEM-Based IoMT Monitoring System*

## 7. Project Requirements

### Functional Requirements

#### FR1: Real-Time Data Collection

- Collect security events from minimum 50 different IoMT device types
- Support for MQTT, HL7 FHIR, DICOM, and TCP/IP protocols
- Real-time data ingestion with latency < 100ms
- Data normalization and standardization capabilities

#### FR2: Alert Prioritization

- Implement machine learning-based threat scoring algorithms
- Integrate clinical impact assessment metrics
- Provide customizable prioritization rules for different healthcare environments
- Support for minimum 10 priority levels with automatic assignment

#### FR3: Alert Grouping

- Correlate related security events within configurable time windows
- Group alerts based on device relationships, attack patterns, and temporal proximity
- Provide visualization of alert clusters and attack campaigns
- Support for manual and automatic grouping rule configuration

#### FR4: Dashboard and Reporting

- Provide real-time security dashboard with customizable views
- Generate automated compliance reports for healthcare regulations
- Support for historical analysis and trend reporting
- Mobile-responsive interface for on-call security personnel

#### FR5: Integration Capabilities

- API interfaces for integration with existing healthcare systems
- Support for standard SIEM integration protocols (CEF, LEEF, Syslog)
- Integration with healthcare incident response workflows
- Compatibility with major cloud and on-premises deployments

### Non-Functional Requirements

#### NFR1: Performance

- Process minimum 100,000 events per second
- Alert prioritization processing time < 500ms
- System availability 99.9% excluding planned maintenance
- Response time for dashboard queries < 2 seconds

**NFR2: Scalability**

- Support for healthcare organizations with 1,000-50,000 IoMT devices
- Horizontal scaling capabilities for increased event volumes
- Cloud-native architecture supporting elastic resource allocation
- Database optimization for historical data storage and retrieval

**NFR3: Security**

- End-to-end encryption for all data transmission
- Role-based access control with healthcare-specific permissions
- Audit logging for all system activities
- Compliance with healthcare cybersecurity standards

**NFR4: Reliability**

- Fault-tolerant architecture with automatic failover
- Data backup and disaster recovery capabilities
- Graceful degradation during component failures
- Comprehensive health monitoring system

**NFR5: Usability**

- Intuitive user interface requiring minimal training
- Customizable dashboards for different user roles
- Comprehensive help documentation and user guides
- Accessibility compliance for healthcare environments

**System Requirements**

**Hardware Requirements**:

- Personal development computer with minimum 16 GB RAM
- SSD storage (minimum 500GB) for development environment
- Additional external storage (1TB) for data and backups
- Raspberry Pi devices (3-4 units) for IoMT device simulation
- Basic networking equipment for testing

**Software Requirements**:

- Linux-based virtual machines (Ubuntu 22.04 LTS)
- Docker containerization platform (free version)
- Open-source SIEM stack (ELK Stack - Elasticsearch, Logstash, Kibana)
- Apache Kafka for stream processing (open source)
- Python 3.9+ and Java 17+ runtime environments
- Open-source machine learning frameworks (TensorFlow, Scikit-learn)

**Development Environment**:

- Git version control system
- Integrated Development Environment (VS Code or PyCharm Community)
- Virtual machine software (VirtualBox or VMware Player)
- Database systems (PostgreSQL, MongoDB - open source versions)

**User Requirements**

**Primary Users**:

- Healthcare cybersecurity analysts
- Hospital IT administrators
- Medical device technicians
- Healthcare compliance officers

**User Capabilities Required**:

- Basic understanding of cybersecurity concepts
- Familiarity with healthcare IT environments
- Ability to interpret security alerts and reports
- Knowledge of healthcare compliance requirements

**Training Requirements**:

- 8-hour initial system training program
- Ongoing professional development workshops
- Technical documentation and user manuals
- 24/7 technical support availability

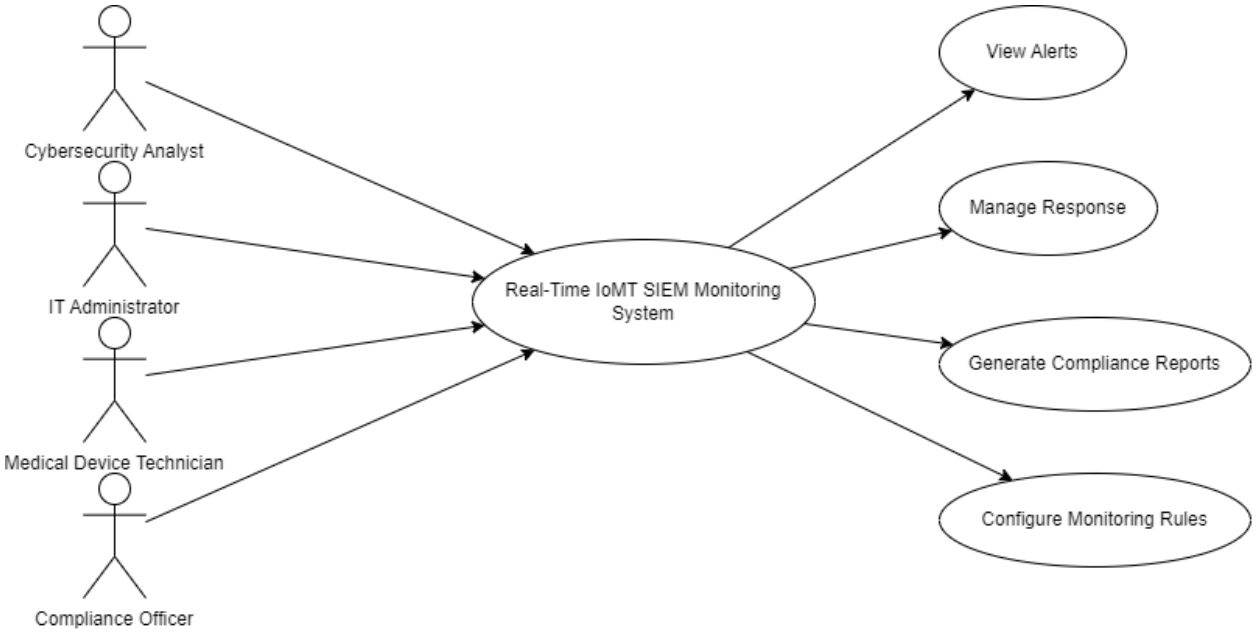



*Figure 4: Use Case Diagram of IoMT SIEM Monitoring System with Primary Users*

## 8. Budget and Budget Justification

Total Project Budget: LKR 175,000

**Budget Breakdown**

**Hardware and Equipment (45% - LKR 78,750)**

- **Development Computer/Laptop**: LKR 45,000
    - High-performance laptop with minimum 16GB RAM and SSD storage
    - Required for development, testing, and running virtual environments
- **IoMT Device Simulators and Testing Equipment**: LKR 20,000
    - Raspberry Pi devices for IoMT device simulation
    - Network equipment for testing (switches, routers)
    - USB devices and sensors for realistic IoMT environment creation
- **Cloud Computing Resources**: LKR 13,750
    - AWS/Google Cloud credits for scalability testing
    - Virtual machine instances for distributed system testing
    - Storage and computing resources for machine learning model training

**Software and Tools (25% - LKR 43,750)**

- **Development Software and Licenses**: LKR 25,000
    - Professional IDE licenses (IntelliJ IDEA, PyCharm)
    - Academic licenses for specialized software
    - Database management tools
- **Open Source SIEM Platform Setup**: LKR 10,000
    - ELK Stack (Elasticsearch, Logstash, Kibana) setup and configuration
    - Apache Kafka for stream processing
    - Grafana for advanced visualization
- **Machine Learning and Analytics Tools**: LKR 8,750
    - Python libraries and frameworks
    - TensorFlow/PyTorch for model development
    - Data analysis and visualization tools

**Research and Documentation (20% - LKR 35,000)**

- **Literature Access and Research**: LKR 15,000
    - IEEE Xplore and ACM Digital Library access
    - Industry reports and cybersecurity threat intelligence feeds
    - Academic journal subscriptions
- **Documentation and Presentation**: LKR 10,000
    - Technical documentation tools
    - Presentation software and templates
    - Academic writing assistance tools
- **Validation and Testing Resources**: LKR 10,000
    - Penetration testing tools and licenses
    - Performance monitoring software
    - User interface testing platforms

**Miscellaneous and Contingency (10% - LKR 17,500)**

- **Internet and Communication**: LKR 7,500

- High-speed internet connection for cloud access and research
- Communication tools for stakeholder engagement

- **Contingency Fund**: LKR 10,000
    - Unexpected expenses and risk mitigation
    - Additional hardware or software requirements

## Budget Justification

**Hardware Investment Rationale**: The 45% allocation to hardware reflects the need for robust development environment capable of running complex SIEM systems and machine learning models. The investment in IoMT simulators enables realistic testing without requiring access to expensive medical equipment.

**Software and Platform Costs**: The 25% software allocation focuses on essential development tools and platforms, emphasizing open-source solutions to minimize costs while maintaining professional development standards. Cloud resources provide scalability testing capabilities within budget constraints.

**Research Foundation**: The 20% research allocation ensures access to current literature and industry insights necessary for developing innovative solutions. This investment supports evidence-based development and contributes to the academic rigor of the project.

**Risk Management**: The 10% contingency allocation provides flexibility for unexpected requirements while maintaining fiscal responsibility appropriate for student research projects.

## 9. Gantt Chart

**Project Timeline: 12 Months**

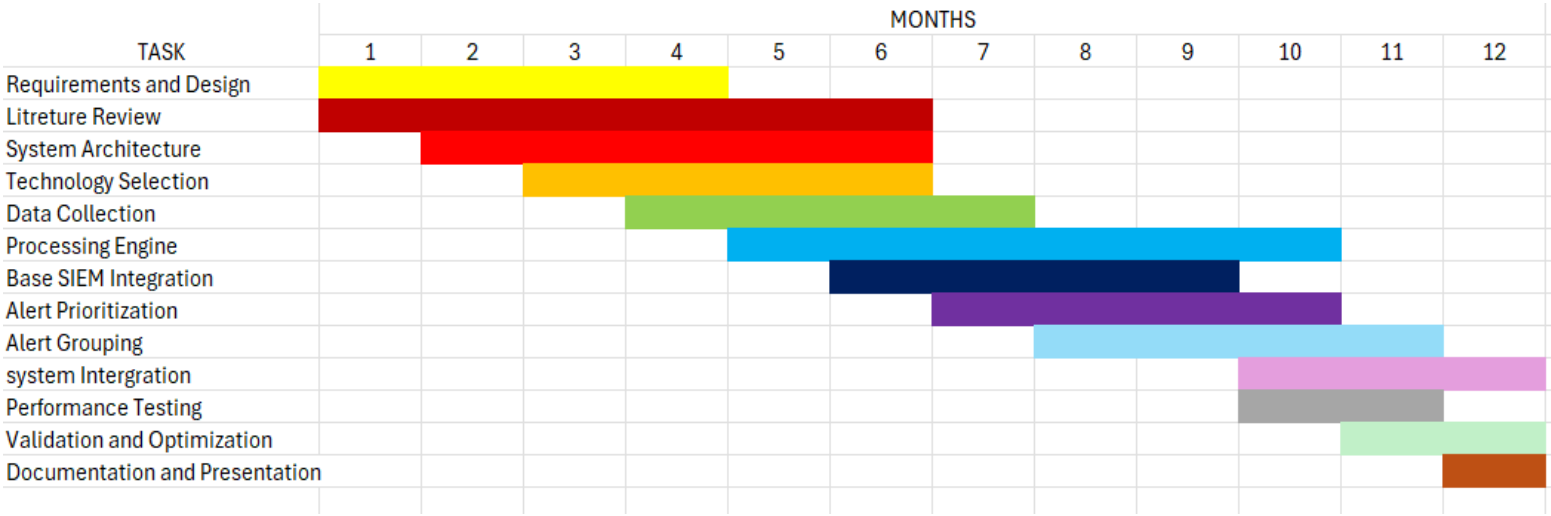



*Figure 5: Project Timeline and Key Milestones (12 Months)*

## 10.References


[1] H. M. P. K. D. A. Z. K. T. A. A. G. S. Dadkhah, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Data in Brief,* vol. 56, 2024.

[2] A. A. S. S. F. Alsubaei, "IoMT malware detection using edge computing and machine learning," *Computers & Security,* vol. 138, 2024.

[3] A. S. D. P. R. Kumar, "Intelligent alert correlation in SIEM systems: A machine learning approach," *Computers & Security,* vol. 139, 2024.

[4] K. T. F. A. D. Robinson, "SIEM architecture optimization for healthcare environments," *Computers in Biology and Medicine,* vol. 172, 2024.

[5] P. A. S. T. X. Liu, "Alert fatigue mitigation strategies in healthcare cybersecurity operations centers," *Health Informatics Journal,* vol. 30, no. 2, 2024.

[6] B. M. C. R. A. Garcia, "Machine learning-based threat prioritization for medical device security," *IEEE Transactions on Biomedical Engineering,* vol. 71, no. 8, 2024.

[7] J. A. S. e. al., "A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks," *Frontiers in Medicine,* vol. 12, 2025.

[8] K. B. J. W. M. Thompson, "Predictive analytics for cybersecurity incident response in healthcare environments," *Journal of Medical Internet Research,* vol. 26, no. 4, 2024.

[9] P. O. S. K. A. Murphy, "Compliance-driven security monitoring for healthcare organizations," *Health Technology,* vol. 14, no. 3, 2024.

[10] J. C. S. R. K. Foster, "Regulatory compliance automation in healthcare cybersecurity monitoring," *Regulatory Affairs Professionals Society Journal,* vol. 29, no. 4, 2024.

[11] L. J. N. W. T. Miller, "Healthcare cybersecurity framework integration: Challenges and solutions," *International Journal of Medical Informatics,* vol. 185, 2024.

[12] Q. L. M. Z. W. Chen, "Behavioral analysis for IoMT anomaly detection using ensemble learning," *Expert Systems with Applications,* vol. 238, 2024.

[13] M. G. P. B. C. Brown, "Threat intelligence integration in healthcare SIEM systems," *Cybersecurity,* vol. 7, 2024.

[14] X. W. Y. L. L. Zhou, "Multi-protocol security assessment frameworks for IoMT environments," *Computer Networks,* vol. 243, 2024.

[15] J. K. P. S. S. Wong, "Graph-based alert correlation for IoT security management," *IEEE Internet of Things Journal,* vol. 11, no. 12, 2024.

[16] G. M. R. E. J. Cooper, "Automated incident response orchestration in healthcare cybersecurity," *Computers & Security,* vol. 140, 2024.

[17] R. D. M. C. E. Johnson, "Adaptive resource management in real-time security monitoring systems," *Computers & Electrical Engineering,* vol. 118, 2024.

[18] D. H. B. M. L. Watson, "Performance optimization techniques for large-scale security event processing," *Journal of Network and Computer Applications,* vol. 219, 2024.

[19] H. T. T. S. K. Yamamoto, "Edge computing integration for IoMT security monitoring," *IEEE Transactions on Industrial Informatics,* vol. 20, no. 7, 2024.

[20] M. A. C. W. R. Taylor, "Cost-benefit analysis of advanced SIEM implementations in healthcare," *Health Economics,* vol. 33, no. 8, 2024.

[21] A. L. D. C. P. Roberts, "Human factors in cybersecurity alert management for healthcare environments," *Applied Ergonomics,* vol. 16, 2024.

[22] S. K. R. G. V. Patel, "Real-time stream processing for cybersecurity event analysis," *Future Generation Computer Systems,* vol. 152, pp. 234-248, 2024.

[23] C. P. Y. K. H. Lee, "Privacy-preserving security monitoring in IoMT networks," *IEEE Transactions on Information Forensics and Security,* vol. 19, 2024.

[24] M. H. N. A. R. Ahmed, "Federated learning for collaborative IoMT threat detection," *IEEE Communications Magazine,* vol. 62, no. 5, pp. 89-95, 2024.

[25] K. V. V. S. A. Singh, "Explainable AI for cybersecurity alert analysis in healthcare," *Artificial Intelligence in Medicine,* vol. 148, 2024.