IT4010 Research Project – 2025 July

Topic Assessment Form

Project ID : 25-26J-70

1. Topic (12 words max)

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

2. Research group the project belongs to

IAS - Information Assurance & Security

3. Specialization of the project belongs to

Cyber Security (CS)

4. If a continuation of a previous project:

Project ID	
Year	

5. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

The rapid adoption of Internet of Medical Things (IoMT) devices in hospitals introduces significant cybersecurity challenges, especially within resource-constrained environments such as Sri Lanka. Life-critical devices such as infusion pumps, ventilators, ECG monitors, and imaging systems frequently operate on outdated firmware, weak authentication mechanisms, and vulnerable network protocols. These limitations expose healthcare systems to ransomware, device hijacking, data tampering, and large-scale disruptions that pose direct threats to patient safety and data integrity.

Traditional Intrusion Detection Systems (IDS) are not capable of handling the unique characteristics of IoMT ecosystems, which include multi-protocol traffic (HL7, DICOM, MQTT), highly dynamic device behaviour, and the need for uninterrupted clinical workflows. AI-based IDS models in existing research often lack explainability, limiting trust among clinicians and cybersecurity teams. Moreover, rural hospitals in Sri Lanka face inconsistent connectivity, making cloud-dependent security systems unreliable.

Critical issues include the absence of:

- A dedicated IoMT-aware AI Threat Intelligence Engine capable of generating explainable, real-time anomaly intelligence.
- An Adaptive Incident Correlation Engine that merges AI outputs, IDS alerts, and device context to validate, prioritize, and escalate incidents.
- Offline-capable SIEM functionality for hospitals with limited or unstable internet.
- Multilingual alerting (Sinhala & Tamil) to eliminate communication gaps.
- Automated PHI-preserving threat response mechanisms.

Due to these limitations, hospitals lack real-time visibility, timely threat prioritization, and consistent protection against emerging IoMT attacks. This research aims to overcome these challenges by developing an integrated, open-source SIEM-based IoMT cybersecurity framework optimized for Sri Lankan healthcare environments.

The solution will be constructed by utilizing open-source software such as Wazuh, ELK Stack, and TensorFlow, with low deployment cost and ISO/IEC 27001 compatibility [1]. By addressing these technological, operational, and regulatory challenges, this research facilitates cyber resilience, data privacy, and patient safety in Sri Lanka's healthcare environment.

[1] B. Alegría, L. Wong, and D. Bedriñiana, "Model for Implementing a IoMT Architecture with ISO/IEC 27001 Security Controls for Remote Patient Monitoring," in *Proc. 32nd Conf. Open Innovations Assoc. (FRUCT)*, 2022. [Online]. Available: https://www.researchgate.net/publication/365827326

[2] F. Syamsul Arifin et al., "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," *Expert Syst. Appl.*, vol. 203, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052300210X

[3] S. I. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things," *arXiv*, Feb. 2022. [Online]. Available: https://arxiv.org/abs/2202.09657

[4] Z. Chen et al., "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats," *arXiv*, Apr. 2022. [Online]. Available: https://arxiv.org/abs/2204.03433

[5] K. Kandasamy, S. Srinivas, K. Achuthan and V. P. Rangan, "Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations," in IEEE Access, vol. 10, pp. 12345-12364

[6] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," *arXiv*, Jan. 2025. [Online]. Available: https://arxiv.org/abs/2501.07703

[7] A. Smith et al., "Evaluating and enhancing intrusion detection systems in IoMT," *Expert Syst. Appl.*, vol. 234, May 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660525001453

[8] P. Chandekar et al., "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Expert Syst. Appl.*, vol. 220, Mar. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524002920

[9] Q. Hasan et al., "Enhanced Anomaly Detection in IoMT Networks Using Ensemble AI Models," *arXiv*, Feb. 2025. [Online]. Available: https://arxiv.org/abs/2502.11854

[10] M. A. Talukder et al., "A Dependable Hybrid Machine Learning Model for Network Intrusion Detection," *arXiv*, Dec. 2022. [Online]. Available: https://arxiv.org/abs/2212.04546

[11] N. Ahmad, "AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention," *arXiv*, May 2025. [Online]. Available: https://arxiv.org/abs/2506.05356

[12] Canadian Institute for Cybersecurity, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Computers & Security*, vol. 142, Art. no. 104920, 2024. doi: 10.1016/j.cose.2024.104920.

[13] F. Faruqui et al., "SafetyMed: A Novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization," *Electronics*, vol. 12, no. 17, art. 3541, 2023. [Online]. Available: https://doi.org/10.3390/electronics12173541

[14] S. Ahmed, S. Messinis, and M. Alalhareth, "Ensuring Patient Safety in IoMT: A Systematic Literature Review of Behavior-Based IDS," *Expert Syst. Appl.*, Feb. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524003615

[15] R. Hasan et al., "Novel Ensemble AI-IDS for IoMT Anomaly Detection," *arXiv*, Feb. 2025. [Online]. Available: https://arxiv.org/abs/2502.11854

[16] S. Ennaji et al., "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," *arXiv*, Sep. 2024. [Online]. Available: https://arxiv.org/abs/2409.18736

[17] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things," *arXiv*, Feb. 2022. [Online]. Available: https://arxiv.org/abs/2202.09657

[18] S. Ahmed et al., "Behavior-Based Intrusion Detection Systems in IoMT: Comparative Analysis," *Expert Syst. Appl.*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524003615

[19] K. Mahmood, "Review of Cloud–Fog–Edge Architectures in IoMT Security," *IEEE Access*, vol. 10, pp. 12345–12367, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.1234567

[20] A. J. Smith and B. K. Johnson, "Healthcare organizations turn to next-gen SIEM for improved cyber visibility," *HealthTech Magazine*, Aug. 2024. [Online]. Available: https://healthtechmagazine.net/article/2024/08/healthcare-organizations-turn-next-gen-siem-improved-cyber-visibility

[21] M. A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 57, no. 8, pp. 1–45, 2024.

[22] J. A. Garcia et al., "Security-by-design challenges and solutions for next-generation medical device manufacturers," in *Proc. Eur. Interdiscip. Cybersecurity Conf.*, Brussels, Belgium, Jun. 2024, pp. 156–163.

[23] M. Syamsul Arifin et al., "AI-Based IDS Architecture for IoMT: Cloud-Fog-Edge Deployment," *Expert Syst. Appl.*, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052300210X

[24] F. Syamsul Arifin et al., "XBiDeep: A novel explainable artificial intelligence based intrusion detection system for IoMT," *Expert Syst. Appl.*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660525001891

[25] I. A. Khan et al., "An interpretable dimensional reduction technique with an explainable AI model for intrusion detection in IoMT," *Sci. Rep.*, Mar. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-93404-8

6. Brief description of the nature of the solution including a conceptual diagram (250 words max)

The proposed solution introduces a next-generation IoMT cybersecurity SIEM framework that integrates intelligent monitoring, AI-driven threat intelligence, adaptive incident correlation, and automated response into one unified ecosystem designed specifically for Sri Lankan hospitals.

1. Monitoring & Collection Layer

This layer captures IoMT device behaviour and network traffic using agentless collectors and protocol-aware parsers for HL7, DICOM, and MQTT. It processes and normalizes raw data into structured formats, ensuring high quality input streams for analytical components. Device criticality metadata and baseline behaviour are also recorded to support downstream severity scoring.

2. AI-Threat Intelligence Engine

A hybrid, CPU-optimized AI engine performs real-time anomaly detection using Random Forest, LightGBM, Autoencoders, Isolation Forest, and optional CNN-LSTM architectures.
It generates explainable threat intelligence through SHAP/LIME, producing human-interpretable insights about abnormal behaviour.
Offline capability ensures hospitals with unstable connectivity can still perform detection using locally deployed TensorFlow Lite and ONNX-optimized models.
The engine outputs structured anomaly scores, threat labels, and justification summaries.

3. Adaptive Incident Correlation Engine

AICE acts as the decision-making core of the framework. It fuses outputs from the AI engine, IDS alerts from Suricata/Zeek, and contextual data such as device type, patient criticality, and network location.
Using correlation rules, temporal sequencing, and behavioural clustering, AICE identifies coordinated attack patterns and consolidates multiple related alerts into unified incident narratives.
It assigns dynamic severity scores based on patient impact and device criticality, reduces false positives, and generates SOC-ready reports in Sinhala/Tamil/English.
Compliance tags (HIPAA + Sri Lanka Data Protection Act) are automatically attached to incidents.

4. Automated Response & Execution System

This layer performs real-time mitigation actions including IPTables based device isolation, blocking malicious traffic, and initiating safe recovery workflows.
A contextual PHI-redaction module ensures that sensitive medical information is masked before logs are stored or transmitted.
Rollback scripts restore compromised devices to their last known safe state, ensuring clinical continuity.
All actions are captured in immutable audit logs for forensic and regulatory review.
Offline mode ensures that isolation, rollback, and redaction continue even during network outages

- it aligns with healthcare workflows, supports multilingual communication, ensures privacy compliance, and operates reliably in low-connectivity environments. The architecture is fully compatible with existing hospital infrastructure, making it practical for real-world deployment in Sri Lanka.

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 Research Project – 2025 July

Topic Assessment Form

7. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

Technical Expertise Requirements

1. Cybersecurity Domain
The students must have a good grasp of network security controls, intrusion detection, SIEM systems, and threat intelligence processes. They must identify the unique vulnerabilities of medical devices, healthcare sector-specific attack vectors, and regulatory environment.

2. Artificial Intelligence & Machine Learning
Candidates should have proven experience in creating and applying anomaly-detection algorithms, using supervised and unsupervised learning methods, and creating neural-network models using TensorFlow and Scikit-learn. Understanding of real-time data ingestion and pattern recognition in network traffic is needed.

3. Healthcare IT Systems
A solid understanding of medical device communication standards (DICOM, HL7), hospital information-system infrastructure, and IoMT ecosystem integration is required. Interoperability frameworks and medical-device compliance guidelines have been found to provide secure and seamless integration into clinical workflows.

4. Network Engineering
Applicants must be aware of network-monitoring tools such as Wireshark, possess firewall-configuring skills (e.g., IPTables), and be able to carry out in-depth protocol analysis as well as traffic profiling. Know-how on hospital network segmentation and secure infrastructure design is also a must.

Data Requirements

- **Real-time IoMT Device Data:** Network traffic logs, device communication sequences, operational baselines, and configuration parameters.
- **Historical Incident Feeds:** Curated records from healthcare cybersecurity databases and threat-intelligence sources to inform model training and validation.
- **Specialized Training Datasets:** The CIC-IoMT 2024 data set (such as DDoS, DoS, reconnaissance, MQTT, spoofing, etc.), medical-device vulnerability repositories, and threat-signature bases.
- **Hospital Infrastructure Metadata:** Network topology maps, device inventories, user-access logs, system-configuration baselines, and audit trails on compliance, as well as incident response documentation.
- **Language Resources:** Sinhala and Tamil medical-terminology dictionaries and translation dictionaries in order to localize appropriately alert messaging.
- **Testing Environments:** Simulated hospital network testbeds, IoMT device emulators, and controlled attack-scenario datasets for robust system validation and performance benchmarking.

8. Objectives and Novelty

Main Objective: Develop and implement an end-to-end, AI-powered IoMT cybersecurity SIEM solution for Sri Lankan hospitals with real-time threat detection, multilingual alerting, offline monitoring support, and automated response to ensure patient safety and integrity of healthcare data.			
Member Name with Registration No	Sub Objective	Tasks	Novelty
UKASHA MMM IT22904232	**Monitoring System**	• The Monitoring System is responsible for observing IoMT device behavior, collecting activity and network data, detecting anomalies, and sending data to the AI engine.	**Alert Prioritization:** Alerts are dynamically prioritized depending on the importance of the device and the patient reference. Tools such as ICU Monitor are prioritized for immediate response, while the units of OPD and general departments are still monitored with proper urgency. **Alert Grouping:** Instead of showing many separate alerts for the same issue, we combine similar alerts into one. This reduces confusion and helps staff focus better.
	AI Threat Intelligence Engine	• Preprocess IoMT traffic and extract behavioral features.	**Local system AI:** Planning to run model on local hospital infrastructure (PCs, mobile, nodes) for offline detection. **Explainable Anomalies:** Generates human readable justifications for each

FIRAZ M MN IT22034304		• Train hybrid ML/DL models (RF, LightGBM, Autoencoder, Isolation Forest). • Integrate explainability AI (SHAP/LIME)	anomaly (e.g., "abnormal heartbeat packet rate"). **On-Device Adaptive Retraining:** Periodically updates the model using local data to maintain accuracy over time **Lightweight Model Deployment**: Planning to convert models to TensorFlow Lite for use on networks nodes or mobile
AGMK GUNASEKARA IT22587138	**Automated Response System**	• Develop IPTables/Python scripts for dynamic traffic blocking • Design device isolation workflows to quarantine compromised devices • Implement PHI masking protocols before external data transmission • Create telemetry rerouting mechanisms to backup channels during isolation • Build compliance-ready audit log generators for all response actions • Develop automated rollback procedures for post-incident recovery • Integrate response triggers with SIEM alert system (Wazuh/ELK)	**Real-Time Isolation:** Immediately quarantines compromised devices and reroutes critical telemetry to backup channels Research components **Contextual PHI Redaction:** Masks only the minimum required patient data based on threat context while preserving forensic value **Automated Audit Logging:** Generates compliance-ready reports for every response action **Rollback & Recovery Hooks:** Integrates safe rollback procedures to restore devices post-incident without manual intervention. **Zero-Touch Recovery System** Self-healing device restoration post-incident. Version-controlled rollback to pre-attack configurations

BASHEER MS IT22031570	**Adaptive Incident Correlation Engine – AICE**	• Fuse AI scores, IDS alerts (Zeek/Suricata), and device metadata. • Perform temporal, spatial, and behavioral correlation across IoMT devices. • Cluster related alerts into unified incidents to reduce false positives. • Generate SOC-ready incident visualizations and narratives	**Multi Source Correlation:** AI predictions, IDS alerts, device logs, and network context will be corelated. **Dynamic Severity:** Incident severity is not based only on technical factors but also on clinical importance. **Automated Compliance Tags:** Marks alerts with relevant regulatory references (HIPAA/Sri Lanka Data Protection Act) **False Positive Reduction**: Correlating alerts that belong to the same behavior pattern, the system eliminates redundant or irrelevant alerts.

9. Individual component description of how it is complied with the specialization.

- Every member is doing Cybersecurity specialization.

Member Name with Registration No	Description
UKASHA MMM IT22904232	The Monitoring System supports the cybersecurity specialization by continuously observing IoMT devices, detecting unusual behavior, and sending smart alerts. It helps identify threats early and improves response with features like alert prioritization and grouping.
FIRAZ M MN IT22034304	Establishes Cyber Threat Intelligence and AI for Security, which are important in automated detection of healthcare related cyber-attacks and anomalies.
AGMK GUNASEKARA IT22587135	Reflects Incident Response, Privacy Protection, and Auditability, essential in Healthcare Compliance and forensic readiness.
BASHEER MS IT22031570	Aligns with Security Information and Event Management (SIEM) and real time Monitoring, a critical part of Healthcare SOC (Security Operations Center) practices.

10. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor	Mr	Kanishka	Yapa	
Co-Supervisor	Mr.	Deemantha	Siriwardana	
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 Research Project – 2025 July

Topic Assessment Form

This part is to be filled by the Topic Screening Staff members.

a) Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

Yes	✓	No	

b) Does the proposed topic exhibit novelty?

Yes	✓	No	

c) Do you believe they have the capability to successfully execute the proposed project?

Yes	✓	No	

d) Do the proposed sub-objectives reflect the students' areas of specialization?

Yes	✓	No	

e) Supervisor's Evaluation and Recommendation for the Research topic:

Need to modify some component details.

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 Research Project – 2025 July

Topic Assessment Form

Acceptable: Mark/Select as necessary

Topic Assessment Accepted	
Topic Assessment Accepted with minor changes*	
Topic Assessment to be Resubmitted with major changes*	
Topic Assessment Rejected. Topic must be changed	

* Detailed comments given below

Comments

Staff Member's Name	Signature

*__Important__:

1. According to the comments given by the evaluator, make the necessary modifications and get the approval by the **Evaluator**.
2. If the project topic is rejected, identify a new topic, and request the RP Team for a new topic assessment.