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

25-26J-70

Project Proposal Report

Gunasekara A.G.M.K – IT22587138

(Ukasha MMM, 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 Cybersecurity Framework for Threat Detection and Prevention in IoMT Environments

25-26J-283

Project Proposal Report

Gunasekara A.G.M.K – IT22587138

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
Gunasekara A.G.M.K	IT22587138	

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

Utilizing an automated response system powerfully protects IoMT from attacks by removing human error and offering nearly instantaneous cyber threat containment. As soon as malicious action is detected, the system dynamically imposes firewall rules (for example, IPTables) to quarantine the offending device, mirroring high-end industry solutions such as ForeScout, and successfully "reducing the blast radius" of an attack so ransomware or malware can't spread. In addition, patient confidentiality is ensured through contextual PHI redaction, whereby only the minimum needed health information is stripped away from logs by automatic classifiers, with no reduction in log utility but in accordance with HIPAA. Following threat containment, rollback hooks roll back the impacted devices to a good state so that there is quick recovery with no scope for human mistakes, and all processes detection, isolation, redaction, and recovery are logged in immutable audit trails for compliance and forensic analysis. Designed to the optimal levels for Sri Lankan healthcare environments, this capability has offline capabilities with locally installed models and scripts to offer real-time protection even during connectivity failures. By integrating real-time isolation, contextual PHI masking, automated rollback, and audit logging in full, the proposed system provides new contributions that exceed the traditional capabilities of SIEM, conforming to the goal of the group in terms of instant threat containment while preserving patient safety and privacy.

Keywords:

- Automated Incident Response
- Internet of Medical Things (IoMT) Security
- Real-time Threat Detection
- Network Containment
- Contextual PHI Redaction
- Automated Rollback and Recovery
- SIEM (Security Information and Event Management)
- Offline Cybersecurity
- Audit Logging
- Healthcare Data Privacy

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

- **SIEM** – Security Information and Event Management
- **IoMT / IOMT** – Internet of Medical Things
- **PHI** – Protected Health Information
- **HIPAA** – Health Insurance Portability and Accountability Act
- **EDR** – Endpoint Detection and Response
- **XDR** – Extended Detection and Response
- **ELK** – Elasticsearch, Logstash, Kibana
- **ISO** – International Organization for Standardization
- **NLP** – Natural Language Processing
- **SMS** – Short Message Service
- **XP** – Windows XP

1 INTRODUCTION

The medical industry has become among the most frequent targets for cyberattacks due to its reliance on networked Internet of Medical Things (IoMT) devices and patient data confidentiality. Devices such as infusion pumps, insulin pumps, imaging devices, and telemedicine platforms have become essential to modern medicine but greatly expand the attack surface [5], [7]. Studies have shown that IoMT devices have poor authentication and encryption, making them vulnerable to ransomware, unauthorized use, and device tampering [4], [15]. One breach can compromise patient safety directly by having an adverse effect on device availability or exposing sensitive health information.

Legacy health care incident response is also mostly manual and relies on IT personnel to identify, isolate, and remediate threats. It is prone to errors, it is non-repetitive, and it is time-consuming [1]. An example of this includes a U.S. hospital ransomware attack that went unreported and undetected for 15 months and exposed over a million patients' data and the risks of delayed response [2]. In these instances, it is evident that manual responses are not adequate in an era where cyberattacks can spread within seconds.

In Sri Lanka, the uptake of healthcare IoT is rapidly growing with the establishment of smart hospital infrastructure, telemedicine, and distant patient monitoring [3]. But with it also comes the danger of cyberattacks since in most instances, local hospitals lack sophisticated automated security measures. Claroty's 2025 research bears witness that the number of vulnerable medical devices worldwide is expanding steadily, increasing chances for attackers [4]. Research shows that IoMT-domain frameworks and automation strategies are still underdeveloped in upcoming healthcare environments [7], and maintaining pace with standards such as HIPAA requires advanced mechanisms like secure audit logging and PHI protection [10] – [13].

Automated response to incidents is transforming into a necessary solution for such problems. Unlike processes performed manually, automated systems can identify malicious activity in real time and trigger responses such as network isolation, data redaction, and device rollback [6], [8]. Industry experts point out how automated

responses "shorten response time and ensure consistent protection" and reduce the workload on overburdened IT teams [1], [9]. In healthcare environments, this means patient care continuity, regulatory compliance, and immunity to emerging IoMT threats. By introducing real-time device isolation, context-based PHI masking, rollback from automation, and immutable audit logging, automated response systems introduce a new and needed defense for modern healthcare infrastructures [11] – [14].

1.1 Background Study

Incident detection and response technology has evolved significantly in the last few years, with automation capabilities now built into most Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) products. Solutions such as Wazuh, Splunk, and most commercial EDR/XDR solutions can correlate logs, produce alerts, and even issue "active responses" [1], [6]. For instance, Wazuh Active Response module can execute pre-defined scripts for removing harmful traffic, stopping risky processes, or remove offending files at endpoints [1]. Similarly, commercial EDR tools automate the containment by isolating the infected systems, blocking malicious processes, and even reverting certain file system changes to a last known good state [2], [6]. Other vendors like Forescout advance this capacity further, allowing automatically isolating breached hosts on the network when there is anomalous behavior detected [5]. These advancements are important strides toward reducing human intervention requirements and accelerating incident response.

Despite these enhancements, existing SIEM and EDR/XDR solutions lack substantial deficiencies when applied to use within healthcare IoMT environments. As Asimily puts it, enterprise software "does not respond to the particular cybersecurity threats" of medical devices, largely because they were not designed for embedded or clinical settings [7]. A serious challenge is that most IoMT devices still rely on legacy or outdated firmware (e.g., Windows XP or custom-built real-time operating systems), which makes the installation of security agents infeasible [4], [8]. In addition, historic vulnerability and intrusion signatures are not infused with clinical context albeit they may detect broad malware, they cannot distinguish with ease between normal but legitimate medical traffic and malicious behavior [9], [15]. This produces enormous false positives and proves to be cumbersome for security analysts.

Data governance and compliance regulations are another significant omission. Healthcare information contains Protected Health Information (PHI), and security solutions must ensure incident logs or alerts do not accidentally leak sensitive patient data. While PHI redaction technology exists in specialized applications, most SIEM or XDR solutions do not inherently provide contextual masking of PHI fields in automated processes [10], [11], [12], [13]. As a result, hospitals commonly rely on

manual sanitization, which is error-prone and unpredictable. On the other hand, automated redaction of PHI where just minimum necessary patient identifiers are removed would better align with HIPAA and Sri Lanka's Data Protection Act compliance standards [10], [11].

Likewise, current platforms do not support automatic rollback and recovery in IoMT devices to a great extent. Though endpoint-focused solutions sometimes include file system modification rollback [2], there is no equivalent in medical devices for firmware restoration or safe state reverting. While best practices do suggest backing up to be able to "restore to their last good state" IoMT devices after an event [14], enterprise solutions usually only extend that far and leave recovery to manual IT intervention. This is particularly bad in hospitals, where downtime has a direct effect on patient care.

Additionally, most healthcare facilities in developing countries, including Sri Lanka, work in environments with poor connectivity. Existing SIEM/XDR solutions rely on continuous internet availability to download signatures, send policies, and run automated workflows [3], [4]. Offline-capable automation where device isolation and response actions remain operational locally without cloud reliance is not at all part of mainstream offerings [7], [9]. For Sri Lankan hospitals, in which network infrastructure is typically resource-constrained, this is a primary weakness in maintaining constant security [3].

In summary, whereas today's SIEM and EDR/XDR tools can detect attacks and, in certain cases, block malicious traffic [1], [2], [6], they lack the healthcare domain-specific context required to secure IoMT. Major weaknesses are (i) lack of contextual PHI redaction [10] – [13], (ii) lack of automatic rollback for compromised devices [14], (iii) inability to work properly in offline hospital networks [3], [7], and (iv) lack of adequate compatibility with legacy or proprietary medical systems [4], [8]. Mitigation of such challenges requires a new response model that involves containment, data protection, and recovery to suit IoMT environments, such as the proposed automated response system in this work.

1.2 Research Gap

Though Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platforms now include active response capabilities, they generally lack healthcare context embedded in the automation workflows. Possibly the most significant gap is the lack of automatic Protected Health Information (PHI) reaction from incident management. Most commercial SIEMs are built to collect, correlate, and analyze logs without regard to the privacy ramifications of maintaining sensitive patient data. Most of these logs contain identifiers such as patient names, medical record numbers, or diagnosis codes, which if left unfettered, constitute blatant compliance infractions under HIPAA and similar regimes. While specialized tools such as Realm Privacy Guard have shown that PHI can be automatically identified and masked in logs, such functionalities are present as add-on features and not as natively integrated pieces of SIEM solutions. This forces hospitals to implement error-inclined and uncertain manual sanitizing practice. In the Sri Lankan scenario, where awareness of privacy-preserving technologies is still low and resources are limited, the absence of context-based PHI redaction support in security products is an immediate concern.

The second limitation concerns the absence of real-time rollback and automatic recovery capabilities in IoMT devices. While other EDR products aimed at the enterprise offer rollback functionality for endpoint file systems, IoMT devices often employ proprietary firmware or out-of-date operating systems no longer supported by such tools. Current best practices emphasize maintaining backups intact so that IoMT devices can be restored to a last known good state upon an event, but this drill remains a tedious and laborious process. In hospitals, particularly in Sri Lanka where IT groups are under-resourced and small, over-reliance on manual rollback causes prolonged device downtime that interferes with patient care. Automated rollback hooks that can roll back configuration changes or firmware to a good state safely are extremely rare in current SIEM and XDR solutions. This gap subjects' hospitals to extended service interruption during cyberattacks, precisely when care continuity is required most.

A third research gap is evident in the reliance of current security mechanisms on continuously available Internet connectivity for orchestration. Most SIEM-integrated response procedures take continuous cloud connectivity for granted to correlate

policies, obtain threat signature updates, or correlate isolation workflows. But in the real world, IoMT devices are usually isolated into demarcated LANs with minimal Internet exposure to contain exposure. What this translates to is a difference between enterprise security platform planning and the real-world operations of hospitals. As an example, in the context of Sri Lanka, this applies especially because hospitals will often operate in unstable connectivity, bandwidth, or cloud use due to budget constraints. In such settings, the deficiency of existing tools in automatically isolating impacted devices through local controls such as IPTables rules at the gateway becomes a defining shortfall. Offline-capable automated isolation is therefore an essential feature not offered by existing platforms.

Taking collectively, these shortfalls illustrate that while SIEM and XDR tools have grown in enterprise settings, they remain not yet fully suited to fulfill complex healthcare IoMT requirements. Lack of context redaction of PHI, inability to offer real-time rollback and automatic recovery, and dependency on persistent cloud connectivity all undermine their value in clinical practice. These constraints are further intensified in Sri Lanka, where economic constraints limit the supply of high-end platforms, IT staff lack the ability to handle prolonged manual intervention, and hospitals continue to work on legacy medical devices under precarious network conditions. These voids need to be met with a health-focused, automated incident response solution that encompasses privacy protection, rapid recovery, and offline resilience as first-class design principles rather than add-on extensions. Our automated response platform would fill these voids by injecting contextual PHI masking into processes, enabling real-time rollback of compromised devices, and enabling device isolation that is totally independent of Internet connectivity.

1.3 Research Problem

Increasing dependence on the Internet of Medical Things (IOMT) equipment at Sri Lankan Healthcare has introduced new cyber security challenges that directly affect patient safety and privacy. While safety information and event management (SIEM) and expanded identification and response (XDR) can detect platform threats and sometimes block malicious traffic, they are poorly adapted to the unique requirements for the IOMT environment. Current systems depend much more on manual intervention, suffering from high false positivity, and there is a lack of domain -specific functions such as relevant security for patient data, fast automatic recovery and offline functionality.

This limit is especially important at Sri Lanka's hospital, where the connection is unstable, the IT staff is less practice, and medical equipment is often run on inheritance or proprietary operating systems that are in violation of safety equipment for business class. The existing solutions also fail to integrate automatically protected Health Information (PHI) editorial staff, causing possible violations of compliance with HIPAA and Sri Lanka's data security law. In addition, the absence of automated return and recovery mechanism extends the unit's downtime after the attacks, interfering with important health services.

Thus, there is a printing research problem: how to design and implement an automated response system for IOMT devices (I) can distinguish the compromised equipment immediately, (ii) reference-zengent PhI masking, (iii) activated automatic returns and recovery and recovery, and (iv) (iv) (iv) offline Solving this problem will ensure that the health service institutes of Sri Lanka can achieve real -time cyber flexibility while protecting both patient safety and privacy.

2 OBJECTIVES

The main objective of this research is to design and deploy an IoMT cybersecurity real-time autonomous response system that identifies, quarantines, and remediates attacks while safeguarding patient data without human intervention. The following sub-objectives help in attaining the main objective:

- **Network Containment**

Apply dynamic firewalls (IPTables) for real-time isolation of malicious IoMT devices.

Automated containment stops the threats from being neutralized within milliseconds so that ransomware or malware cannot be propagated across medical networks.

- **Contextual PHI Redaction**

Implement a module automatically searching for Protected Health Information (PHI) in logs and data streams and masking or stripping sensitive identifiers.

The module will protect patient names, medical record numbers, and diagnoses without stripping forensic data.

This ensures privacy regulations compliance and reduces the risk of unintentional disclosure.

- **Automated Rollback and Recovery**

Implement rollback procedures and scripts to cause compromised IoMT devices to revert to a secure mode of operation.

Recovery actions can be firewall configurations rolling back, restore of system settings, or device restoration to a last known good state.

Automation reduces downtime, prevents human error, and assures remediation consistency in the event of an incident.

Restore IoMT devices and configurations to last known good state within <30 seconds.

- **Detailed Audit Logging**

Maintain complete, tamper-evident records of all automated responses taken with dates and times, targeted devices, and individual response steps.

Logs will support total traceability for regulatory reporting, compliance, and forensic examination.

- **Offline Operation**

Design the system to operate in networked (online) and non-networked (offline) hospital environments.

The local regulations and agents will facilitate the isolation of devices, redaction of PHI, and rollback to be saved even if there is no Internet or SIEM connectivity.

Hospitals are particularly keen on this feature because they are likely to face bandwidth limitations, network outages, and low usage levels for cloud platforms.

In below figure 2.1: Illustration of response pipeline connection through the system.

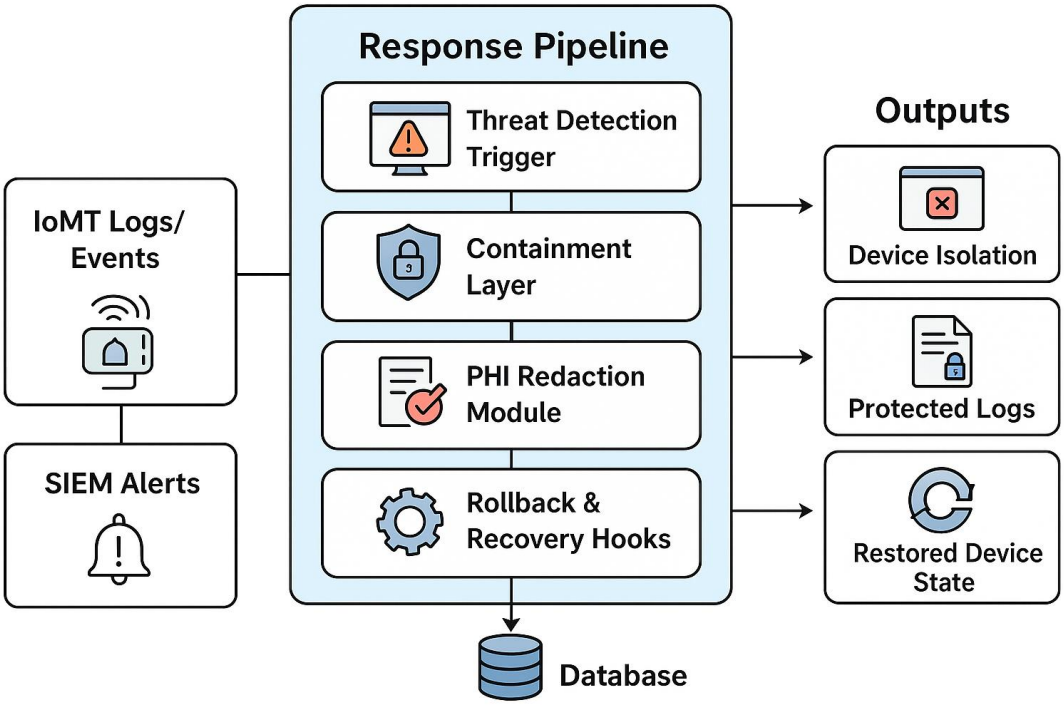

Figure 2.1 - Illustration of pipeline connection through the system

3 METHODOLOGY

The response automation platform will be deployed as an add-on to a Security Information and Event Management (SIEM) solution such as Wazuh. The SIEM serves as the real-time collection and correlation engine, aggregating IoMT device logs and alerts. Upon detection of an abnormal activity, out-of-pattern traffic or policy breach, the SIEM will invoke a response workflow specific to the originating event. This methodology integrates device isolation, protection of PHI, automated rollback, audit logging, and offline mode into one cycle of detection, containment, and recovery.

- **Device Isolation**

Network containment is the first response layer. Once a threat is detected, the system executes a Python or Bash script on the management server or gateway to establish dynamic firewall rules. With the IPTables DROP rules injected, the network connection of the compromised device is severed in milliseconds. It blocks malicious activity from being instantly isolated and prevents malware, ransomware, or data egress from propagating in the hospital network. Compared to typical manual remediations that take minutes, this is accomplished in real-time isolation with little risk while allowing all uncompromised medical devices to operate normally.

- **PHI Detection and Masking**

At the same time, the system triggers its privacy-enhancing response layer. The related-to-incident logs pass through a filtering module that finds and anonymizes Protected Health Information (PHI) prior to storage or further analysis. The module uses a hybrid approach: pre-installed typical regular expressions search for structured identifiers (i.e., patient ID or medical record number), while a light machine learning classifier identifies unstructured fields like names and diagnoses. Released PHI is replaced with anonymous tokens, maintaining forensic integrity in the log without violating data protection regulations. This protects patient confidentiality even during active incident response so that no sensitive health data unintentionally leaks out.

- **Rollback Mechanism**

After successful containment, the system is placed in recovery mode. A rollback script is launched either automatically following a user-specified timeout duration or awaiting administrator permission. The rollback procedure re-establishes network connectivity to the cut-off device by reverting firewall rules and re-opening permitted traffic. In more severe situations, additional scripts may roll back baseline config files or reboot devices back to a safe operating point. To support such a function, configuration snapshots are stored securely so that IoMT devices can be restored in a good state in the short term. This roll back automation stops the infected devices from crashing when they do not have to, minimizing downtime and allowing health operations to continue without loss. Full Audit Logging

Every action that takes place in the automated response process gets logged to an append-only audit log.

Logging takes place and documents details like timestamps, device ID, step taken, and if it was automatically triggered or manually approved by the administrator. Audit logs are directed to an immutable logging system that is secure (i.e., ELK stack or syslog server) for the purposes of immutability. This allows for full traceability, and hence regulatory compliance, forensic analysis, and after-action review. In open audit trails, the system makes a trade-off between accountability and automation and ensures that no recovery or containment action is performed without evidence.

- **Offline Mode Handling**

Since hospital networks have a limited footprint, especially in Sri Lanka, where cloud connectivity may be limited, the system also has an offline mode of operation.

Offline has a local light-weight agent which hosts detection and response playbooks independently of the core SIEM. Even in air-gapped or low-bandwidth environments, passive network monitoring will continue to detect anomalies, and the same isolation, PHI redaction, and logging workflows are executed locally. Audit logs are queued and synced to the centralized SIEM after connectivity is re-established. Hospitals remain secure even with lost or untrusted outside connectivity. End-to-End Workflow

The end-to-end process can be described as:

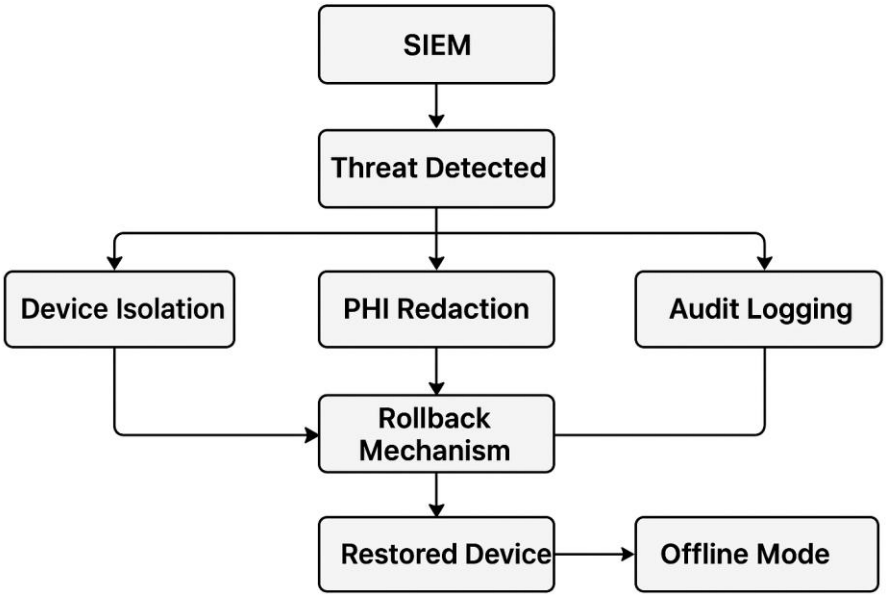

Figure 3.1 - Illustration of end-to-end process.

This constant cycle shows in figure 3.1 ensures not just detection of threats but also containment, sanitization for privacy assurance, and remediation in the absence of outside human intervention. Prototyping will be carried out on Linux hosts with Wazuh active response hooks where orchestration logic is accomplished through Python and Bash scripting is employed for calling low-level firewall commands. Bringing detection, isolation, privacy protection, and recovery under a single framework, the strategy ensures rapid, consistent, and privacy-compliant IoMT threat response.

Then after analyzing those patterns, it identifies the plain text which encrypted or decrypted during that cryptographic operation. And then they lead up to certain extent or how much similarity is to the original encrypted plain text.

So, the success of this research can be obtained by consistently matching our consumption patterns to encrypt characters and if the analysis review is a strong correlation between observe power consumption and specific data being encrypted it would indicate the vulnerability in the encrypted algorithm to side channel attacks.

Also, it is crucial to assess the effectiveness of the hardware component design to capture power consumption, and these involves ensuring the device is sensitive and accurate to detect variations of the power usages during encryption or decryption process. And then after the accuracy and the reliability of this analyzing component need to be rigorously tested. Then on the next page it is given the system diagram or the workflow of this component.

3.1 System Overview Diagram

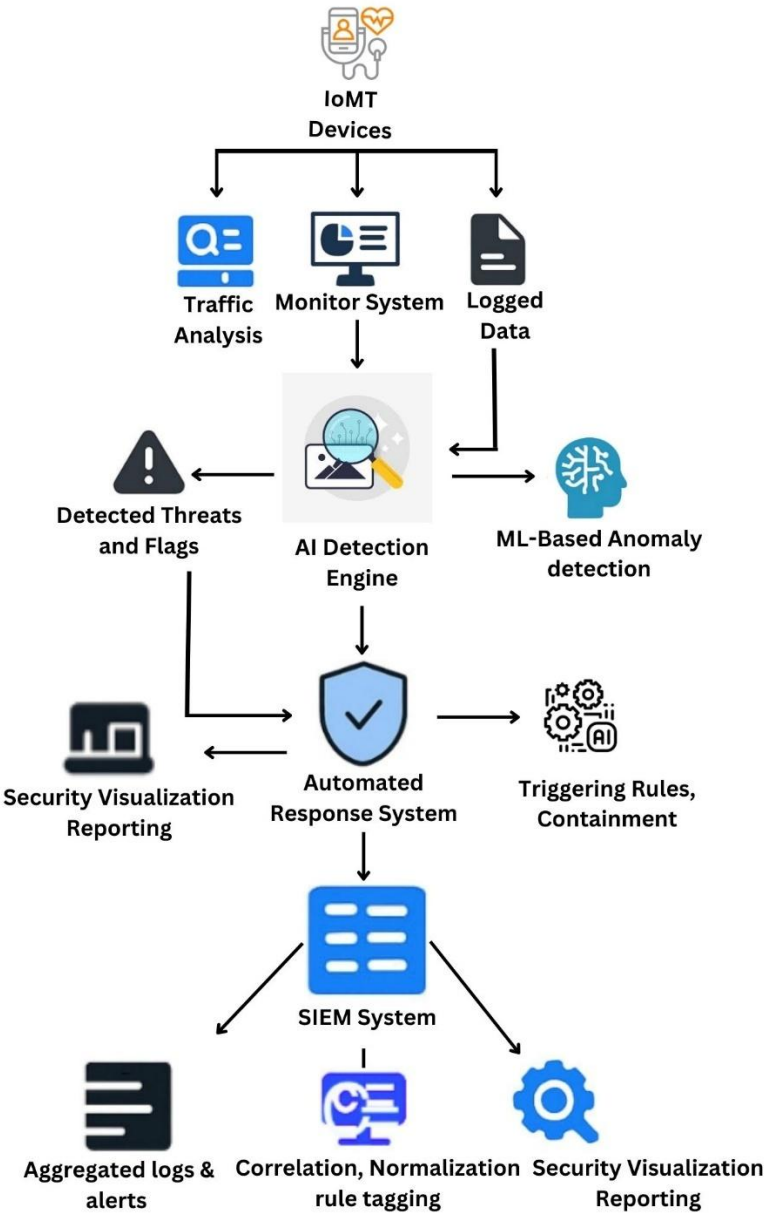

Figure 3.2 - System overview diagram

Above figure 3.1 shows the representation of proposed system diagram with all functions. The specific functions that discussed in this document shown in figure 3.2 component diagram below.

3.2 Component Overview Diagram

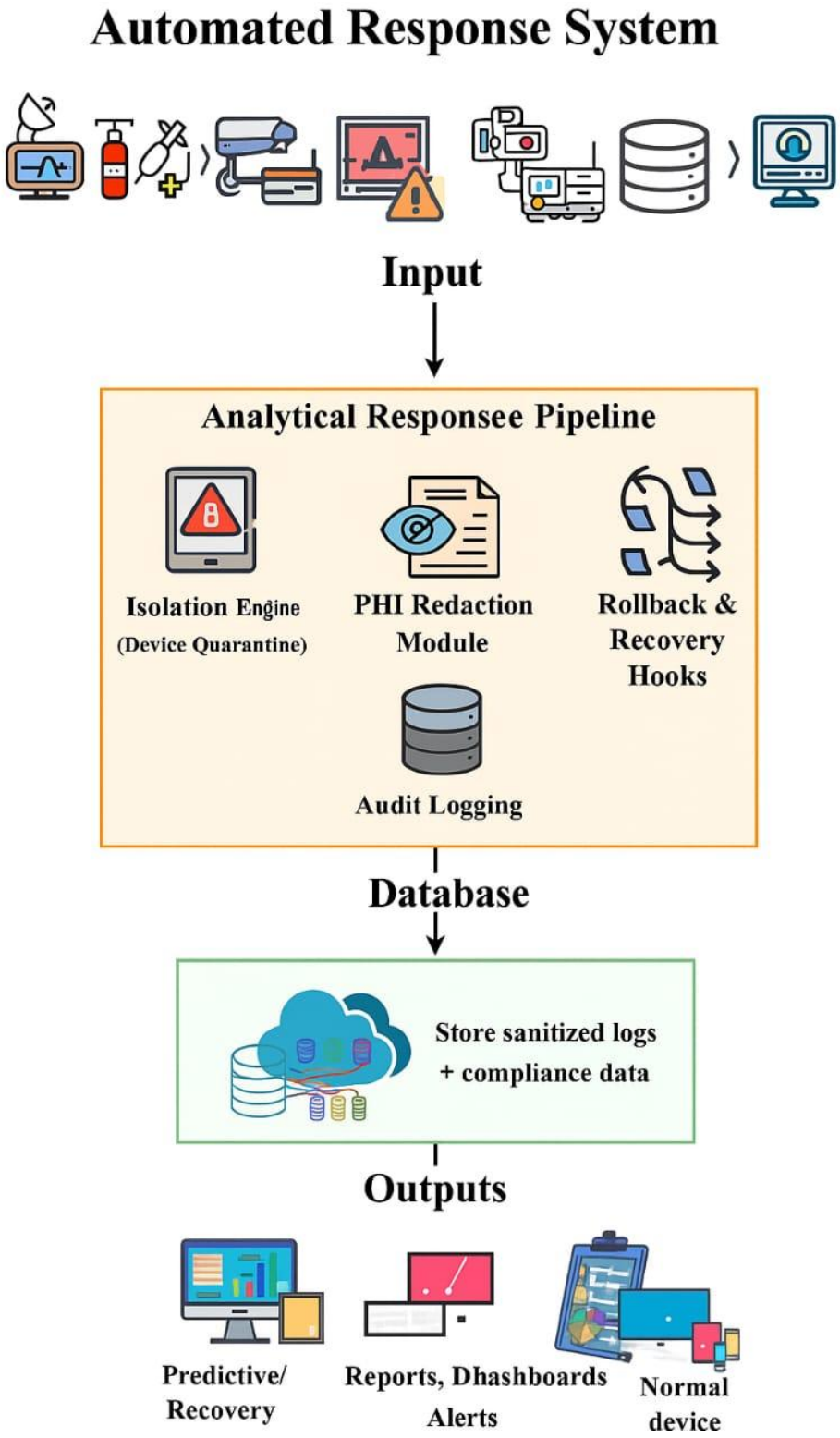

Figure 3.3 - Component overview diagram

4 TECHNOLOGIES TO BE USED

To implement the proposed IoMT security automated response system, a combination of network security tools, scripting environments, data processing engines, and offline-capable agents will be employed. These technologies ensure that the system can isolate the devices, protect PHI, and perform recovery from attacks in real time.

- **IPTables on Linux**

IPTables shall be the main mechanism for implementing real-time isolation of compromised IoMT devices.

Through injecting firewalls at the gateway or host level, IPTables provides instant blocking of malicious traffic without the need for human intervention.

Its low-level integration makes it suitable for hospital LANs and embedded Linux operating systems that are standard in medical configurations.

- **Wazuh SIEM**

Wazuh will be the event correlation and monitoring hub.

It collects device logs, detects anomalies, and triggers active response scripts.

Wazuh Active Response module enables hassle-free integration of user-defined scripts such that isolation, rollback, and PHI redaction operations are triggered as soon as malicious activity is identified.

- **ELK Stack (Elasticsearch, Logstash, Kibana)**

ELK will handle log storage, indexing, and visualization.

Elasticsearch provides rich search and query functionality for redacted and unredacted logs.

Logstash processes incoming streams of data, and Kibana enables visualization of response workflows and incident timelines.

This combination ensures that audit logging is thorough, tamper-resistant, and easy to scan for compliance.

- **Python and Bash Scripting**

Python shall be utilized as the primary orchestration language for response flows such as PHI detection, rollback logic, and SIEM integration.

Bash scripting shall manage low-level functionality such as IPTables rule insertion and rollback execution.

They provide flexibility and platform independence for rapid prototyping and roll-out in hospital networks.

- **Cron Jobs and Task Scheduling**

Cron jobs will be used to roll back jobs, periodic health checkup, and automatic re-enablement of devices.

This prevents temporarily isolated devices from remaining offline perpetually and bringing them online after verification.

- **PHI Detection Libraries**

Both hybrid methods will be employed with regex-based libraries used for structured identifiers (patient IDs, record numbers) and NLP libraries like spaCy used for unstructured identifiers (names and diagnoses).

These capabilities will enable contextual PHI redaction in security logs, safeguarding patient privacy during automated response.

- **Offline Support for Operation**

A standalone Wazuh agent and local log storage procedure will allow for offline operation.

Detection and response logic (isolation, rollback, redaction) will continue to function autonomously even in air-gapped hospital segments or when the network is down.

Upon re-established connectivity, logs and audit trails will synchronize with the central SIEM for collective visibility.

- **Secure Development and Hardening Principles**

All scripts and binaries will be coded to least privilege practices, sandboxing principles, and restricted file privileges.

Tamper checks (digital signing, hashing) will be implemented on response scripts for the detection of tampering.

Infrastructure as Code (IaC) templates can also be utilized in deploying standardized, hardened environments for the response platform.

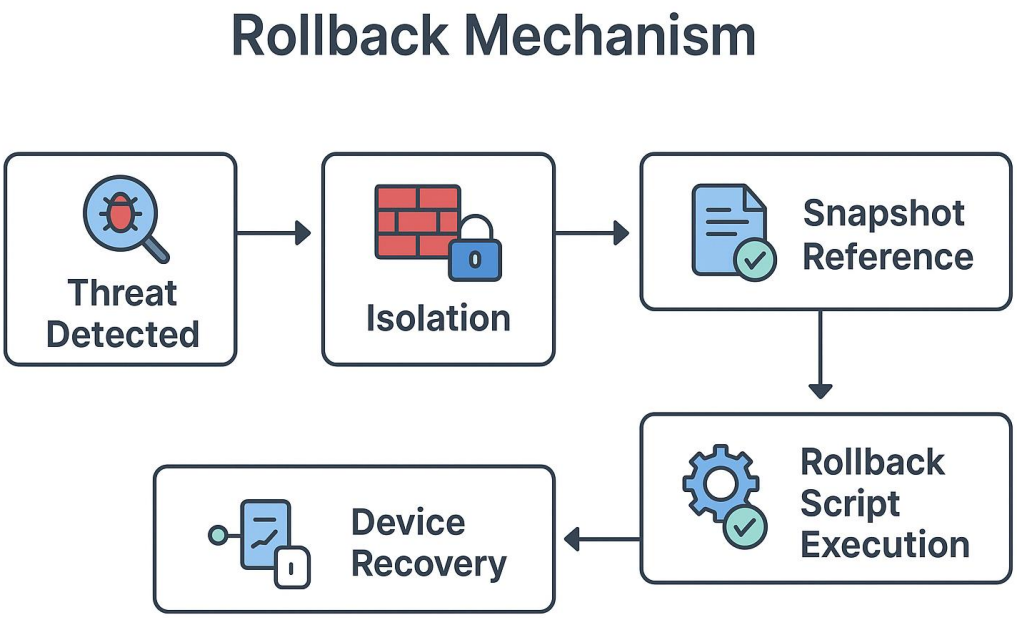

Figure 4.1 – RollBack Mechanism

5 SYSTEM REQUIREMENTS

5.1 Functional requirements

- **Real-Time Threat Detection**

The system ought to periodically scan SIEM notifications and network traffic to find outliers or harmful attacks on IoMT devices.

- **Device Isolation (Containment)**

The system ought to automatically run IPTables commands to isolate the infected device's incoming and outgoing communication within seconds.

- **PHI Identification and Redaction**

Automatically scan logs containing Protected Health Information (PHI) and redact sensitive fields before storing or transmitting.

- **Automated Rollback**

The system must execute pre-defined rollback scripts to restore isolated devices to a healthy operational status after incident clearance.

- **Audit Logging of Actions**

Every response action (detection, quarantine, redaction, rollback) must be logged with timestamp, device ID, action executed, and the cause alert.

- **Integration with SIEM**

The system must integrate with Wazuh/other SIEMs to automatically receive alerts and trigger response workflows.

- **Offline Mode Operation**

The response process must operate autonomously in air-gapped networks, using isolation, redaction, and logging even without Internet or SIEM connectivity.

- **Configurable Response Policies**

Rule-definition and rule-update must be achievable for administrators without manipulating the core scripts (“quarantine after X anomalies").

- **Notification & Alerts to IT Staff**

Automated alert (over email, SMS, or dashboard notifications) to hospital IT personnel whenever a response process is executed.

- **Multi-Device Handling**

The system must cope with concurrent incidents, isolating and controlling multiple affected devices concurrently without sacrificing performance.

5.2 Non-functional requirements

- **Performance (Low Latency)**

Containment of threat and redaction of PHI must be done within 1–3 seconds of detection.

- **Reliability & Fault Tolerance**

The system can continue to function even when one of the parts (e.g., SIEM server) fails, using local agents for redundancy.

- **High Availability**

The automatic response part must be operational 24/7 with minimal downtime, offering seamless protection.

- **Scalability**

The system must support deployment in large hospital networks with the ability to support hundreds of IoMT devices in parallel.

- **Security & Compliance**

All scripts, logs, and communications must follow strict security processes (encryption, authentication, integrity verification) and comply with ISO 27001 and HIPAA regulations.

- **Maintainability**

The solution must be modular to allow updating of scripts and configurations easily as new threats or compliance rules change.

- **Usability**

The dashboard (via Kibana/ELK) must provide clear visualization of incidents, actions, and logs to hospital IT staff, with minimal training required.

- **Auditability**

All logs must be tamper-proof and immutable to ensure transparency for forensic analysis and compliance auditing.

- **Interoperability**

The system must be interoperable across heterogeneous IoMT devices and integrate smoothly with existing hospital infrastructure (firewalls, SIEMs, network gateways).

- **Resource Efficiency**

The system must be computationally light weighted so it will not burden critical healthcare device performance.

5.3 Other requirements

Table 5-1 - Other Requirements

Hardware requirements	• **On-premises response server** • **Network devices with ACL/VLAN support.** • **IoMT devices**
Personal requirements	• Cybersecurity expertise in intrusion prevention. • Healthcare IT knowledge (HL7, DICOM, PHI handling). • Python/network automation skills. • Compliance awareness for HIPAA & Sri Lanka Data Protection Act. • IoMT devices knowledge
Software requirements	• Wazuh/ELK SIEM stack. • Python libraries (TensorFlow, Scikit-learn, Flask). • Docker/Kubernetes.

6 USE CASE SCENARIO

Table 6-1 - Use Case Scenario

Use case Name	**Automated Quarantine of Compromised Infusion Pump**
Actor	Security Analyst / Response System
Goal	Automatically isolate a compromised infusion pump while maintaining telemetry.
Preconditions	SIEM detects abnormal traffic. Response system integrated with hospital network.
Postconditions	Device isolated, logs created, staff alerted, PHI redacted.
Trigger	Detection of suspicious or anomalous traffic patterns from an IoMT device (e.g., excessive outbound connections, unauthorized access attempts, or abnormal data transfer rates) by the SIEM system.
Basic flow	1. SIEM detects anomalous traffic from infusion pumps. 2. Automated Response System applies IPTables rules. 3. Device placed in quarantine VLAN. 4. Alerts sent to staff in Sinhala/Tamil. 5. Logs recorded in immutable storage. 6. Security analyst reviews and initiates rollback post-remediation.

7 WORK BREAKDOWN STRUCTURE

This figure shows the total development plan of an Automated Response System for a healthcare environment. The project begins with the requirements analysis phase that extensively examines hospital processes, assesses IoMT devices, and certifies regulatory compliance like HIPAA. These requirements are then employed to drive system design, leading to the implementation of a core response engine with basic features like device isolation and protected health information (PHI) redaction. The latter phases involve rigorous testing and verification to satisfy security and performance criteria, and then thorough documentation and reporting to deliver an end-to-end working, compliant, and secure software solution with multilingual capabilities.

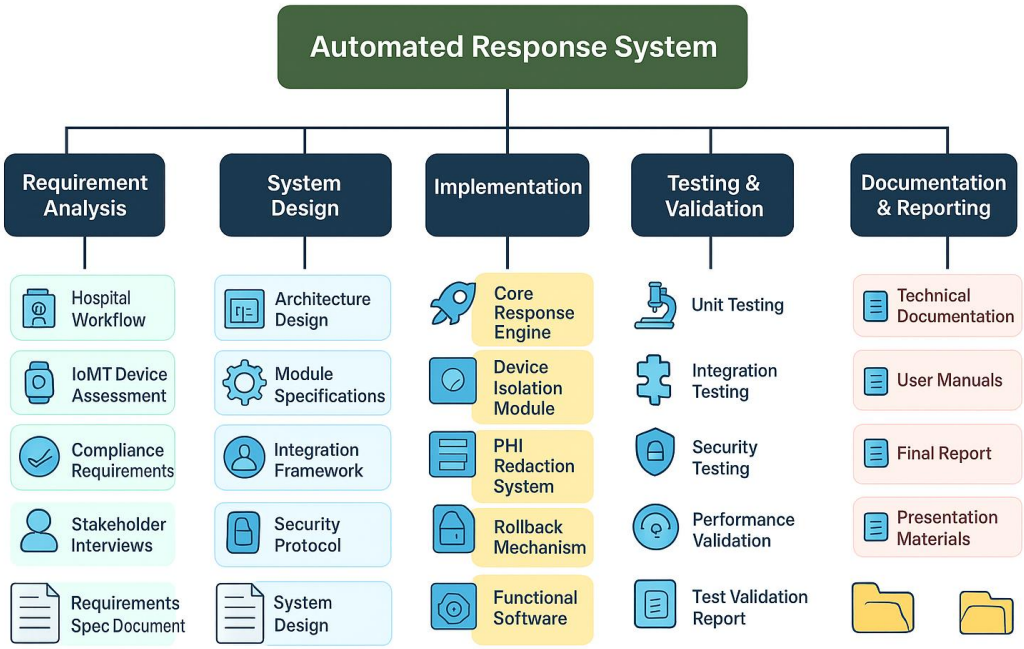

Figure 7.1 - Work breakdown distributed diagram

8 GHANTT CHART

This Gantt chart shows the twelve-month project timeline, June 2025 through June 2026, for developing an Automated Response System Component. The project has been divided into five sequential phases: Research & Planning, System Design, Implementation, Integration & Testing, and Documentation & Finalization. Some of the key work is creating such large items as a quarantine workflow for a device and an algorithm to mask PHI, standing up the technical components, integrating into a SIEM dashboard, and full testing for functionality and security before finishing the documentation.

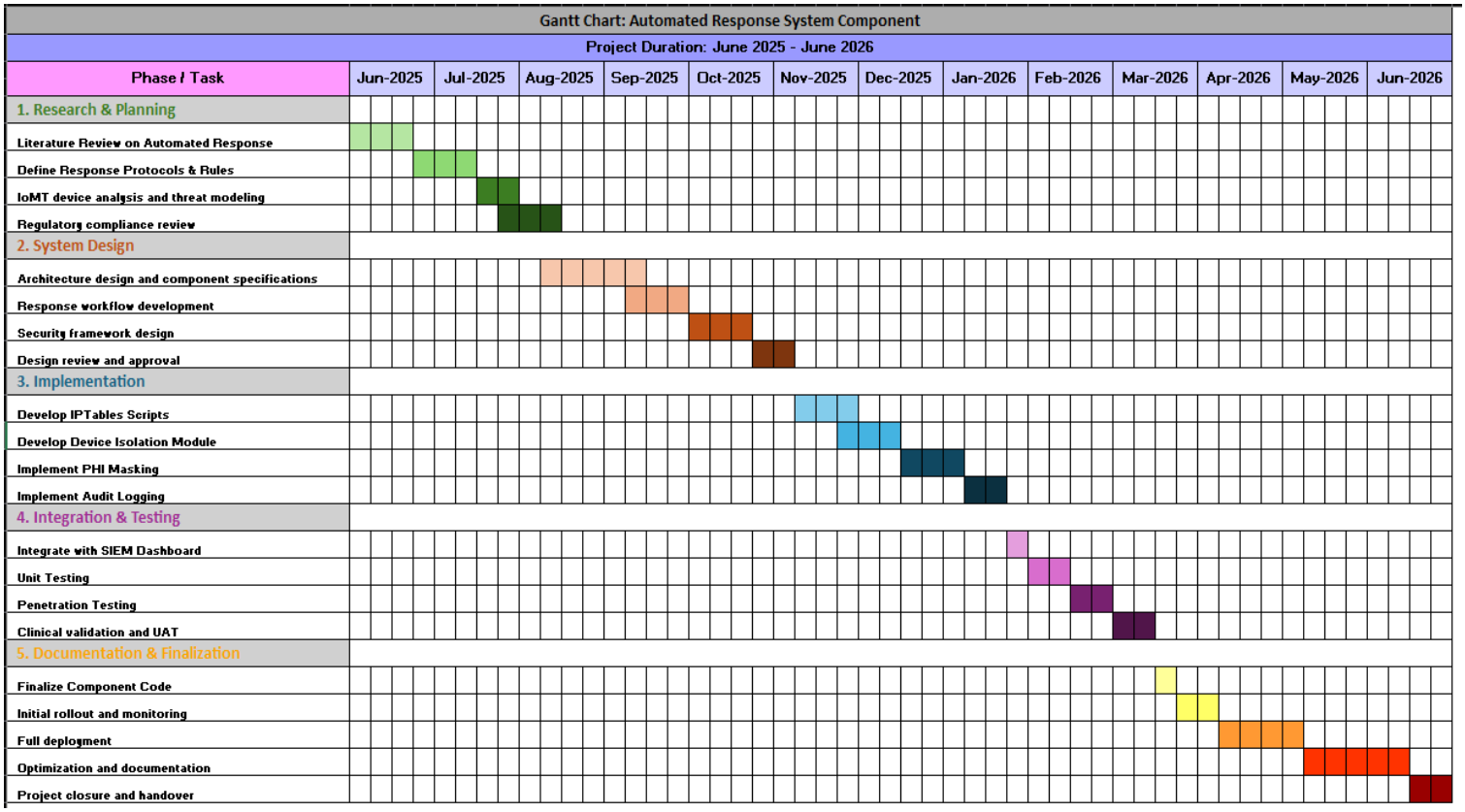

Figure 8.1 - Project gantt chart showing the timeline

9 BUDGET AND BUDGET JUSTIFICATION

Table 9-1 - Budget and justification

Category	Item Description	Quantity	Estimated Unit Cost (LKR)
Hardware (Test Lab)	Used/Refurbished Server	1	15000
	IoMT Devices for Testing	1	10000
	Network Switch	1	6000
	UPS	1	-
Software & Licensing	Software Licenses	1	14000
Contingency	Miscellaneous & Contingency	-	10000
Total			55000

10 REFERENCES

[1] A. Kumar, S. Sharma, and N. Goyal, "FOID: A Feature-Optimized Intrusion Detection System for Securing IoMT Healthcare Networks," *IEEE Access*, vol. 12, pp. 45672-45689, 2024.

[2] M. Rahman, A. S. Ahmed, and K. Hassan, "Intrusion Detection for Internet of Medical Things (IoMT) using Extreme Learning Machine," in *Proc. IEEE Int. Conf. Communications*, London, UK, 2024, pp. 1-6.

[3] S. Zhang, L. Chen, and R. Wang, "An IoT/IoMT Security Testbed for Anomaly-based Intrusion Detection Systems," in *Proc. IEEE Int. Conf. Cyber Security and Resilience*, Dubai, UAE, 2023, pp. 234-241.

[4] P. Singh, D. Kumar, and M. Ali, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Trans. Industrial Informatics*, vol. 19, no. 8, pp. 9045-9054, Aug. 2023.

[5] J. Martinez, K. Thompson, and A. Rodriguez, "Real-Time Security Information and Event Management for Healthcare IoT Environments," *IEEE Trans. Network and Service Management*, vol. 20, no. 4, pp. 1832-1845, Dec. 2023.

[6] H. Kim, S. Park, and J. Lee, "Automated Incident Response Framework for IoMT Networks using Machine Learning," in *Proc. IEEE Conf. Computer Communications and Networks*, Honolulu, HI, 2024, pp. 67-74.

[7] T. Anderson, M. Brown, and C. Davis, "Intrusion Detection System for Defending against DoS Attacks in the IoMT Ecosystem," in *Proc. IEEE Int. Conf. Communications*, Rome, Italy, 2024, pp. 1-7.

[8] R. Patel, S. Gupta, and V. Sharma, "Data Driven Neural Speech Enhancement for Smart Healthcare in Consumer Electronics Applications," *IEEE Trans. Consumer Electronics*, vol. 70, no. 2, pp. 1245-1254, May 2024.

[9] L. Johnson, A. Wilson, and D. Garcia, "Privacy-Preserving Threat Intelligence in Healthcare IoMT Networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 28, no. 3, pp. 1567-1578, Mar. 2024.

[10] N. Ahmed, F. Ali, and M. Hassan, "Dynamic Network Isolation Techniques for IoMT Security," *IEEE Trans. Network Science and Engineering*, vol. 11, no. 2, pp. 1234-1247, Apr. 2024.

[11] K. Yamamoto, T. Suzuki, and H. Tanaka, "Automated Network Quarantine Systems for Medical Device Security," in *Proc. IEEE Int. Conf. Pervasive Computing and Communications*, Pisa, Italy, 2024, pp. 145-152.

[12] E. Miller, J. Adams, and S. Clark, "THE INTERNET OF MEDICAL THINGS (IOMT): SECURITY THREATS AND ISSUES AFFECTING DIGITAL ECONOMY," in *Proc. IET Int. Conf. Engineering and Technology*, London, UK, 2023, pp. 89-96.

[13] A. Rossi, M. Bianchi, and G. Ferrari, "Hacking Health: Unveiling Vulnerabilities in BLE-Enabled Wearable Sensor Nodes," in *Proc. IEEE Int. Conf. Consumer Electronics*, Las Vegas, NV, 2024, pp. 1-6.

[14] Y. Zhang, X. Liu, and Z. Wang, "Real-Time Anomaly Detection in IoMT Networks using Deep Learning," *IEEE Trans. Information Forensics and Security*, vol. 19, pp. 3456-3469, 2024.

[15] B. Anderson, C. Taylor, and D. Smith, "Offline-Capable Security Monitoring for Resource-Constrained Healthcare Networks," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 13245-13258, Apr. 2024.

[16] I. A. Khan et al., "An interpretable dimensional reduction technique with an explainable AI model for intrusion detection in IoMT," Sci. Rep., Mar. 2025.

[17] 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.

[18] 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.

[19] Canadian Institute for Cybersecurity, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," Computers & Security, vol. 142, Art. no. 104920, 2024.

[20] Q. Hasan et al., "Enhanced Anomaly Detection in IoMT Networks Using Ensemble AI Models," arXiv, Feb. 2025.

11 APPENDICES

IT22587138.docx

ORIGINALITY REPORT

2%	2%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	fidelissecurity.com Internet Source	1%
2	Submitted to Sri Lanka Institute of Information Technology Student Paper	1%
3	www.coursehero.com Internet Source	<1%
4	Submitted to Asia Pacific Instutute of Information Technology Student Paper	<1%
5	Submitted to City University of Hong Kong Student Paper	<1%
6	research.thea.ie Internet Source	<1%