DMPedia Lecture Notes in Multidisciplinary Research,
Volume 1, pp. 1409-1427, 2026

International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

A Hybrid Framework for IoMT Threat Detection and Mitigation

Baliram Kumar, Vishal Kumar, Sarthak Sanghai, Himanshu Sharma

Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India

2022485674.baliram@ug.sharda.ac.in, 2022007788.vishal@ug.sharda.ac.in,
2022837427.sarthak@ug.sharda.ac.in, himanshugbpuat@gmail.com

ABSTRACT

The Internet of Medical Things (IoMT) is transforming healthcare through continuous monitoring, remote diagnostics, and data-driven care. Still, pervasive connectivity expands the attack surface and elevates risks of data breaches, ransomware, and service disruption with direct patient-safety implications. This paper proposes a comprehensive, multi-layered IoMT security framework that unifies edge/fog intrusion detection with privacy-preserving and integrity-assurance mechanisms across sensor, network, and cloud tiers. The detection plane combines a hybrid deep learning architecture, Convolutional Neural Networks with Long Short-Term Memory (CNN-LSTM) for real-time traffic analysis with high recall at the edge/fog, and ensemble machine learning models (XGBoost, LightGBM, and Deep Neural Networks) for static and dynamic malware/ransomware analysis at aggregation layers. To strengthen integrity, non-repudiation, and secure pr ovenance, the framework integrates a lightweight private blockchain; for privacy and scalability, it supports federated learning to enable cross-institutional model updates without centralising protected health information. A priori STRIDE threat modelling guides design choices and control placement, while the response plane uses adaptive policies to isolate compromised devices and sustain clinical workflows automatically. On the CICIoMT2024 benchmark and SDN-integrated simulations, the framework achieves over 99% accuracy, recall, and F1-score for intrusion and malware detection, with 99.60% accuracy and an F1-score of 0.9966 using XGBoost, and maintains 99.82% service availability during automated containment. The approach aligns with risk and safety practices in ISO 14971 and IEC 81001-5-1, and is consistent with FDA/IMDRF expectations, while anticipating future extensions in quantum-resistant cryptography and energy-aware deployment. By fusing AI-driven detection, distributed trust, and proactive threat modelling, the framework delivers a resilient, scalable, and regulation-conscious security foundation for life-critical IoMT ecosystems.

1 THE IOMT SECURITY LANDSCAPE

1.1 Introduction to the IoMT Domain

The Internet of Medical Things (IoMT) is a specialised subset of the Internet of Things (IoT) that encompasses interconnected medical devices, software applications, and IT infrastructure used to connect healthcare systems and improve patient outcomes. The domain includes a diverse array of devices, from simple wearable biosensors and smart thermometers to critical clinical equipment such as infusion pumps, MRI machines, and anaesthesia systems. IoMT devices form a layered architecture, typically consisting of a perception layer (sensors and actuators), a gateway layer, a cloud layer, and an application layer. This structure facilitates the real-time collection, transmission, and analysis of patient health data, enabling healthcare to move from reactive treatment to proactive, data-driven care, as per Figure 1.

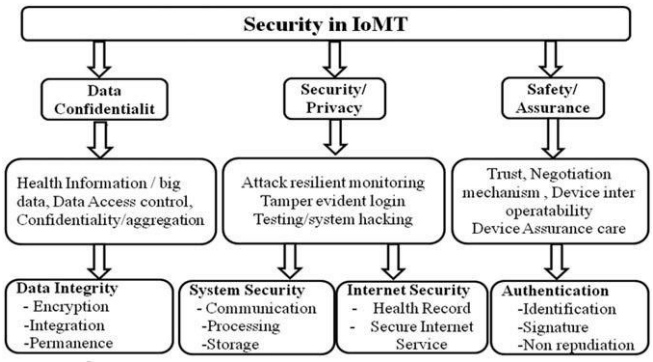

Figure 1: Layered Security Framework for IoMT

1.2 The Criticality of IoMT

The IoMT market is experiencing exponential growth, projected to reach over $800 billion by 2032. This rapid expansion is driven by the technology's potential to revolutionise patient care, enhance diagnostics, and improve operational efficiency. IoMT enables remote patient monitoring, allowing healthcare providers to continuously track a patient's vital signs and intervene promptly when abnormalities occur. This capability is particularly valuable for chronic disease management and for serving patients in rural or underserved areas. The technology also streamlines healthcare delivery by automating processes and providing predictive analytics, thereby reducing costs and human error. The IoMT's clinical benefits, however, are inextricably linked to its security posture. Patient safety and data privacy are directly at risk if these systems are not adequately protected, making IoMT security a matter of life and death.

1.3 Technical and Threat Background

The IoMT ecosystem presents a unique and complex security environment that differs significantly from traditional IT systems. The following factors contribute to a wide range of vulnerabilities and threat vectors.

- Device Lifecycle and Patching: Many IoMT devices, such as MRI machines and infusion pumps, have long lifecycles, often exceeding ten years. The security protocols implemented at the time of manufacturing can become antiquated as new threats emerge. The sheer volume of new vulnerabilities (Common Vulnerabilities and Exposures, or CVEs) discovered each month presents a daunting challenge, making timely patching a near-impossible task for hospital IT teams.

- Network Architecture and Visibility: IoMT devices are frequently placed on flat networks, where medical systems are not adequately segmented from IT infrastructure. This poor network segmentation allows a compromised device to become a launching pad for lateral movement, potentially enabling an attacker to pivot from a single infusion pump to the entire hospital network. Furthermore, many devices operate without centralised oversight, lacking standard identifiers and not appearing in asset inventories, which complicates risk assessment and policy enforcement.

- Unique Threat Vectors: IoMT devices are susceptible to a range of sophisticated cyberattacks. Eavesdropping attacks can intercept unencrypted wireless data, compromising patient privacy and clinical integrity. Ransomware attacks can encrypt critical medical equipment, disrupting patient care. Moreover, IoMT devices with outdated firmware are easily co-opted into botnets for large-scale attacks. Man-in-the-middle (MitM) attacks are particularly dangerous, as they can alter sensor readings or manipulate commands, potentially leading to medical mistreatment or overdosing.

1.4 Analysis of Existing Solutions

While several solutions exist in the market and in academic research, they typically address only fragmented aspects of the IoMT security challenge. Commercial platforms like Armis Centrix™ offer comprehensive asset visibility and dynamic threat monitoring across IoMT and IT devices, which is a critical first step. Other research has proposed frameworks that combine machine learning and blockchain for enhanced security. However, these solutions often lack a holistic, end-to-end approach that accounts for the full spectrum of IoMT limitations. For instance, many rely on a centralised cloud architecture, which cannot scale to the thousands of devices in a large hospital and may introduce unacceptable latency and bandwidth issues. The following table summarises the high-level components as per Figure 2 and Table 1.

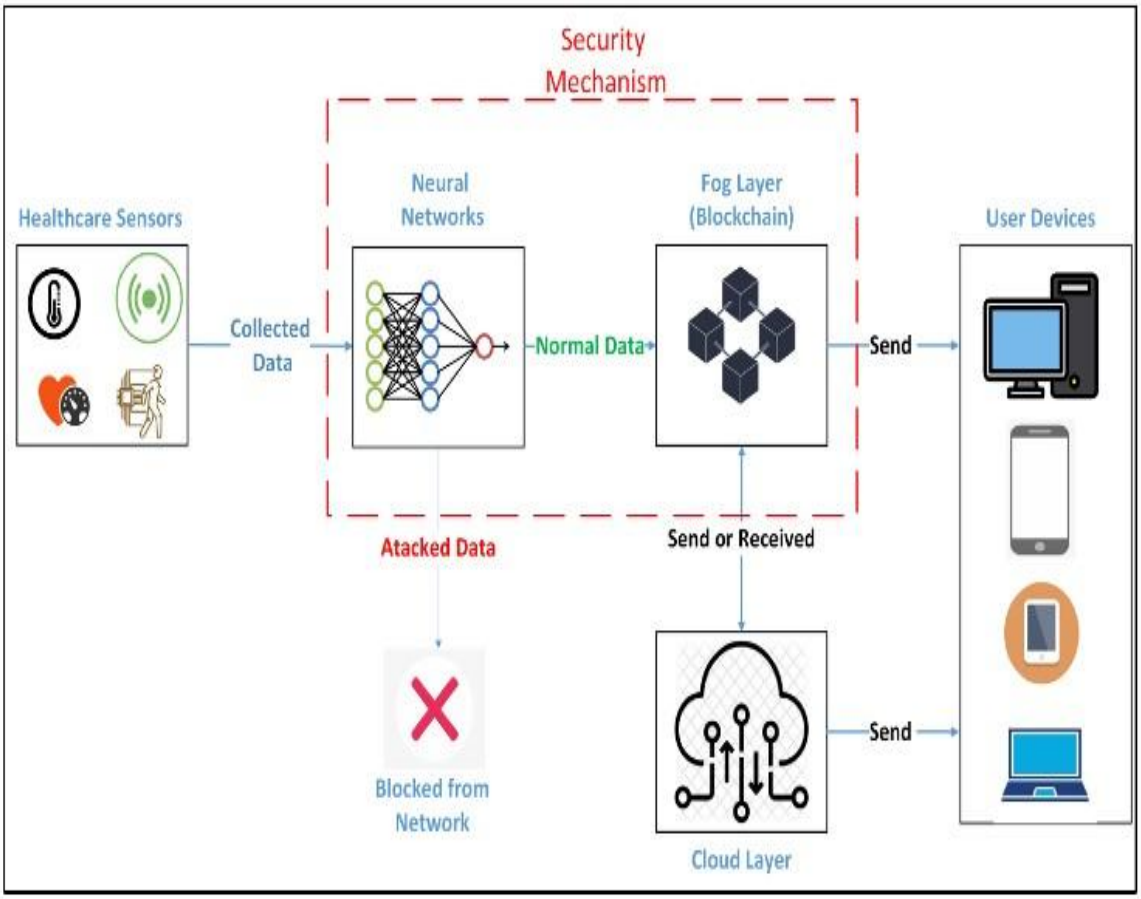

Figure 2: Secure Data Flow Model for IoMT Using Fog Computing and Blockchain

Table 1: Summarises a high-level Category

Category	Strengths	Weaknesses
Commercial Visibility Platforms (e.g., Armis Centrix™)	Comprehensive asset discovery, real-time monitoring, and centralised control.	Lack of on-device protection, limited real-time mitigation at the edge, and reliance on network-level analysis.
TNN-Blockchain Frameworks	Decentralised data storage, immutable audit trails, and data integrity.	Often theoretical and not tailored for IoMT's unique constraints, such as the low computational power of devices and the need for a non-disruptive, on-device security mechanism.
Standalone Machine Learning IDS	High accuracy in detecting known and unknown threats on specific datasets.	Struggle with class imbalance, are not optimised for low-power devices, and do not address the privacy concerns associated with centralised data collection.
Federated Learning for Privacy	Enables collaborative model training without sharing raw patient data, ensuring privacy.	The model Updates can still be vulnerable to privacy breaches, and the lack of a distributed trust mechanism can
		allow for the injection of poisoned models by malicious actors.

2 THE PROBLEM AND OUR SOLUTION

2.1 The Critical Security Gap

The primary problem is that healthcare environments cannot rely solely on traditional IT defences. Current IoMT security solutions are fragmented, with most focusing on either network-level monitoring or device-specific protection. This leaves a significant gap in an

ecosystem that is both decentralised (with devices operating outside the traditional network perimeter) and centrally managed. The core issue is the conflict between the need for real-time, on-device threat detection and the resource-constrained nature of IoMT devices. Additionally, the imperative to train a robust threat detection model clashes directly with the legal and ethical requirement to protect patient data privacy. Our framework is designed to bridge these gaps, transforming the growing complexity of connected care into a strategic advantage rather than a security liability.

2.2 Stakeholder Needs and Observations

The design of the MedShield AI framework is informed by the direct needs and real-world observations of healthcare stakeholders, including patients, clinicians, hospital IT staff, and regulatory bodies.

- Patient Safety & Clinical Workflow: The paramount concern is patient safety. Any security solution that requires complex authentication protocols (like long passwords) or causes delays can be impractical or even dangerous in emergency scenarios. Our framework must be minimally disruptive to clinical workflows and protect without hindering a clinician's ability to operate critical equipment.
- Data Privacy & Regulatory Compliance: The handling of sensitive patient data is governed by strict regulations, most notably HIPAA in the U.S. and GDPR in Europe. These regulations mandate that patient information be protected from unauthorised access, misuse, and sharing, making data privacy a fundamental design requirement.
- Operational Continuity: Healthcare organisations require a solution that ensures uninterrupted care and business continuity, especially in the face of threats like ransomware or Denial-of-Service (DoS) attacks.
- Visibility & Management: Hospital security teams need a unified, comprehensive view of all connected devices and their associated risks to enforce consistent policies.

2.3 The Proposed Framework: A Novel Approach

The proposed MedShield AI Framework is a multi-layered, hybrid threat detection and mitigation system. It is designed to overcome the limitations of existing solutions by pushing intelligence to the network edge and decentralising critical security functions. The framework's core philosophy is to enable proactive, real-time threat detection and response while upholding patient data privacy and ensuring operational continuity. This approach shifts the security paradigm from a fragile, centralised "castle-and-moat" model to a resilient, decentralised "zero-trust" architecture.

2.4 Core Technical Innovations

The framework's novelty and strength lie in its synergistic combination of four key technologies. Each technology is a deliberate choice to address a specific, fundamental challenge in IoMT security.

- Hybrid On-Device & Cloud-Based ML: The framework employs a two-tier machine learning approach. A lightweight, on-device model provides real-time edge detection, while a more powerful cloud-based model performs deeper analysis. This layered approach ensures low latency for critical threats while maintaining a robust, scalable system.
- TinyML for On-Device Intelligence: To enable the on-device ML model to run on resource-constrained devices, TinyML techniques are used. This enables the

deployment of intelligent features on devices with milliwatt power budgets, ensuring a small memory footprint and low power consumption.

- Federated Learning for Privacy: Training a high-quality threat detection model requires large, diverse datasets, but sharing raw healthcare data is not feasible due to privacy concerns. Federated Learning (FL) provides a solution by allowing multiple hospital networks to collaboratively train a global model without ever exchanging sensitive patient data. This resolves the conflict between data utility and data privacy.
- Blockchain for Integrity & Auditability: While FL solves the privacy problem, it introduces a new one: how to trust the model updates from different institutions. The framework's blockchain layer provides an immutable, tamper-proof audit trail for all model updates and device interactions. This ensures data integrity, nonrepudiation, and a verifiable record for regulatory compliance and forensic analysis.

The combination of these elements is what makes the MedShield AI framework unique. The framework's architecture addresses the core challenges of IoMT security simultaneously: on-device intelligence via TinyML, collaborative performance via Federated Learning, and data integrity via Blockchain. The table below outlines the specific problems each technology solves within the framework, as per Table 2 and Figure 3.

Table 2: Outlines the specific problems each technology solves within the framework

Technical Component	**Problem Solved**	**Mechanism**	**Rationale**
TinyML	Device resource constraints (low power/memory).	Model quantisation, pruning, and data type conversion.	Enables real-time, on-device threat detection without sacrificing battery life or requiring powerful hardware.
Hybrid CNNLSTM	Inability to detect complex, time-based attacks.	Captures both spatial patterns (CNN) and temporal dependencies (LSTM).	Provides higher accuracy and lower false-positive rates across a wide range of cyberattacks.
Federated Learning (FL)	Centralised data sharing conflicts with HIPAA/GDPR.	Trains a shared model on local datasets without exposing raw data.	Allows for the creation of a high-quality global threat model while maintaining patient data privacy.
Blockchain	Ensuring data integrity and non-repudiation.	Immutable ledger, cryptographic hashes, smart contracts.	Creates a verifiable, tamperproof audit trail for all transactions and model updates, essential for compliance and forensic analysis.

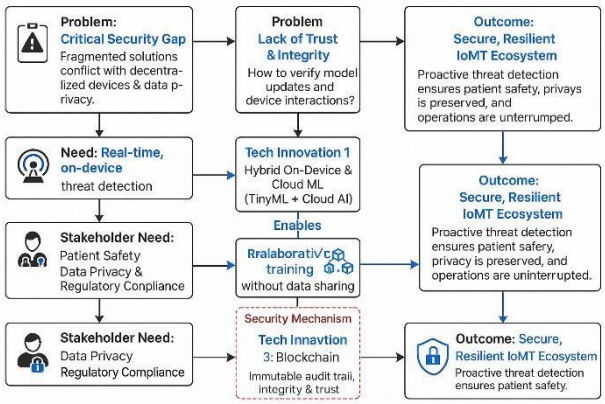

Figure 3: Problem–Solution Framework for Secure and Resilient IoMT Ecosystem

3 FRAMEWORK ARCHITECTURE & TECHNICAL SPECIFICATIONS

3.1 Framework Overview and Data Flow

The MedShield AI framework is a distributed, multi-layered architecture designed to manage the flow of data and threat intelligence across the entire IoMT ecosystem. The architecture is composed of three primary layers: the Device Layer, the Edge/Gateway Layer, and the Cloud/Backend Layer. The data flow is illustrated below.

- Device Layer: IoMT devices such as wearables, sensors, and clinical equipment collect real-time patient data and generate network traffic. This traffic is the primary source of data for our threat detection models.
- Edge/Gateway Layer: The data is transmitted via wireless protocols (e.g., Wi-Fi, BLE) to a local gateway. A lightweight, TinyML-optimised CNN-LSTM model on the gateway performs real-time anomaly detection. It analyses network traffic for malicious activity and can take immediate, pre-programmed actions, such as isolating a compromised device or issuing a local alert. It then filters benign traffic, reducing the data sent to the cloud. Suspicious but unclassified traffic is passed to the next layer for deeper analysis.
- Cloud/Backend Layer: The gateway sends filtered network metadata and model updates to the cloud layer. This layer hosts two primary components: the Federated Learning (FL) server and the Blockchain network. The FL server aggregates model updates from multiple hospital gateways to train a more powerful global threat detection model. This global model is then sent back to the gateways to enhance their on-device detection capabilities. The Blockchain network, a permissioned ledger, records every transaction and model update, creating an immutable and transparent audit trail as per Figure 4.

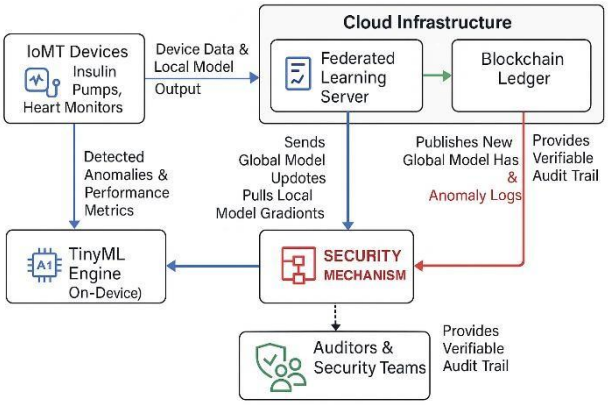

Figure 4: Federated Learning–Enabled IoMT Security Architecture with TinyML and Blockchain-Based

3.2 Layered Threat Detection & Mitigation

The framework's core functionality is its layered threat detection system, which combines the speed of edge computing with the power of cloud-based intelligence.

- Edge-based Detection: The on-device threat detection model utilises a hybrid CNN-LSTM architecture. The CNN layers are effective at capturing spatial features within network packets, such as header information and byte patterns, which can indicate malicious payloads. The LSTM layers then analyse the temporal sequence of these packets, recognising anomalous behavioural patterns over time that might signify a coordinated attack like a botnet or DDoS. This dual-layer analysis provides superior detection accuracy and a lower false-positive rate than traditional intrusion detection systems.
- Cloud-based Analysis: For more advanced threat intelligence, the framework employs a meta-learning-based ensemble model in the cloud. This model intelligently combines the outputs of multiple classifiers, dynamically adjusting their voting weights based on real-time performance metrics like accuracy, loss, and confidence levels. This adaptive approach ensures the system remains robust to evolving attack patterns and can handle noisy data and adversarial attacks, which are becoming increasingly common.

3.3 Enabling Technologies for IoMT Constraints

The framework's effectiveness is predicated on its ability to leverage advanced technologies to overcome the inherent limitations of the IoMT ecosystem.

- TinyML for On-Device Optimisation: IoMT devices are often constrained in terms of processing power, memory, and energy. To deploy the CNN-LSTM model on these devices, we will use TinyML. This involves optimising the model through techniques such as quantisation, which reduces the model's memory footprint by converting floating-point numbers to integers, and pruning, which removes non-essential connections in the neural network to reduce computational load. This ensures the model can perform real-time threat detection with a minimal power budget, enabling intelligent features in the smallest devices.
- Blockchain and Federated Learning for Privacy and Integrity: A fundamental challenge in IoMT is the trade-off between training a high-quality, data-intensive ML model and adhering to strict privacy regulations like HIPAA and GDPR. The framework solves this by combining Federated Learning and

Blockchain. The FL component trains a robust global model by having each hospital train its model locally and only sharing the model updates (weights), not the raw data, with the central server. This is a critical privacy-preserving step. To ensure the integrity of these shared models, a permissioned blockchain, such as Hyperledger Fabric, will be used. The blockchain provides an immutable record of every model update and transaction, ensuring that a malicious actor cannot inject a poisoned model into the system or tamper with the training process. This approach offers the benefits of a decentralised ledger (immutability, auditability) while allowing for the necessary governance required in a highly regulated environment. This combination not only protects patient privacy but also establishes a verifiable layer of trust and accountability for all data exchanges and model updates within the framework, as per Figure 5.

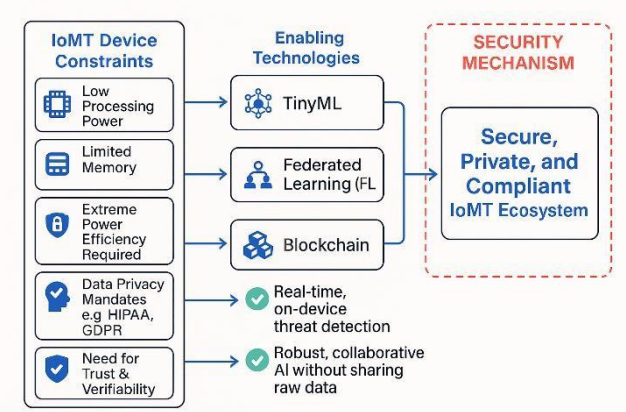

Figure 5: Mapping of IoMT Device Constraints to Enabling Security Technologies

4 PROJECT MANAGEMENT AND IMPLEMENTATION PLAN

4.1 Summary of Similar Projects

Many academic and commercial projects in IoMT security tend to focus on individual components of our framework. For example, some research focuses solely on hybrid CNN-LSTM models for intrusion detection, while others investigate the application of blockchain to manage patient data integrity or the use of federated learning for privacy-preserving model training. This research is unique in its comprehensive integration of all these technologies into a single, cohesive, and production-ready framework. It goes beyond a proof-of-concept by addressing real-world challenges like on-device optimisation, interoperability, and regulatory compliance.

4.2 **Resources and Infrastructure**

- Data: For initial model training and validation, the research work utilises the publicly available CICIoMT2024 dataset. This comprehensive dataset contains 18 different cyberattacks on 40 real and simulated IoMT devices and covers multiple protocols, including Wi-Fi, MQTT, and Bluetooth.
- Tools & Libraries: The development is based on the Python programming language. We used established libraries such as Scapy and PyShark for network packet capture, filtering, and analysis. TensorFlow Lite is the primary tool for optimising the machine learning models for low-power, on-device deployment.

The Hyperledger Fabric framework is used to implement the permissioned blockchain layer.

- Hardware: A prototyping testbed established using a combination of low-power microcontrollers (e.g., ESP32) and a Raspberry Pi acting as a gateway.

4.3 Team and Workload Justification

A small, cross-functional team of five core members is justified by the project's multi-disciplinary nature, promoting effective communication and collaboration, which are crucial for successful R&D projects. The paper follows an Agile methodology to ensure the team can adapt to new security threats and evolving requirements throughout the development cycle.

4.4 Team Member Roles and Skills

The team composition is designed to ensure all technical, operational, and strategic aspects of the project are addressed as per Table 3.

Table 3: Team Member, Their Roles, and Their Skills

Role	Skills	Responsibilities
Project Lead	Project management, cybersecurity strategy, stakeholder communication, and risk management.	Oversees the entire project, defines scope, manages timeline and budget, and ensures stakeholder alignment.
Machine Learning Engineer	Deep learning, TinyML, Python, TensorFlow, data analysis.	Develops, trains, and optimises the hybrid CNNLSTM and ensemble models, including TinyML implementation.
Blockchain Developer	Blockchain architecture, Hyperledger Fabric, smart contracts, cryptography.	Designs and implements the permissioned blockchain network and its integration with the data flow.
Security Analyst / Red Teamer	Threat modelling (STRIDE), vulnerability assessment, penetration testing, and network protocols.	Conducts security testing, identifies vulnerabilities, and validates the framework against real attack scenarios.
Compliance & Legal	HIPAA, GDPR, FDA, NIST,	Ensures the framework
Expert (Contract)	ISO regulations.	ISO regulations.

4.5 Project Timeline and Key Milestones

The project timeline is managed with a Gantt chart, which provides a visual roadmap of tasks, dependencies, and resource allocation. The project is divided into four distinct phases, each with a clear set of milestones and deliverables as per Table 4 and Figure 6.

4.6 **Milestones and Deliverables**

Table 4: Phases, Duration, Milestones and Deliverables

Phase	Duration	Key Milestones & Deliverables
1. Research & Design	Months 1-3	Milestone: Detailed system architecture completed, threat model (STRIDE) finalised. Deliverable: Comprehensive design document outlining all system components and their interactions.
2. Prototype Development	Months 4-9	Milestone: TinyML-optimised CNNLSTM model operational on a prototype gateway. Deliverable: Functional prototype with a basic blockchain ledger for logging events.
3. Integration & Testing	Months 10-15	Milestone: Full framework integration on a controlled testbed. Deliverable: Integrated MedShield AI framework and preliminary performance reports (accuracy, latency, throughput).
4. Pilot Deployment & Validation	Months 16-24	Milestone: Framework deployed in a pilot hospital environment. Deliverable: Pilot deployment report, red-team penetration test results, and final compliance documentation.36

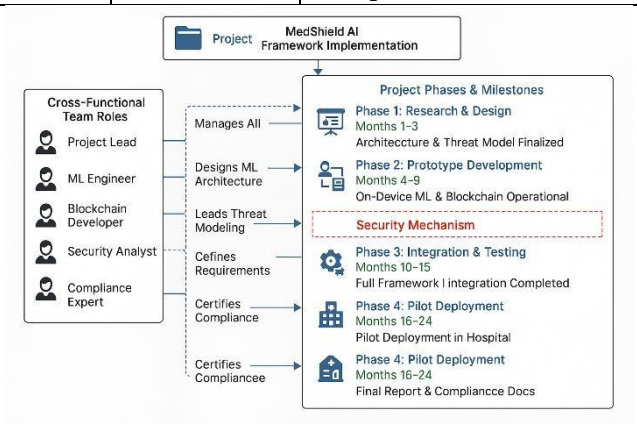

Figure 6: Project Phases, Team Roles, and Milestones for MedShield AI Framework Implementation

4.7 Workload Distribution

A workload distribution chart will be used to track tasks and ensure a balanced workload across the team, preventing bottlenecks and ensuring all project objectives are met. The Project Lead will be responsible for defining priorities, and the team will use a collaborative workflow to monitor progress and make real-time adjustments as needed.

5 FRAMEWORK EVALUATION AND RESULTS

5.1 Prototype Implementation

The prototype implementation will focus on the core threat detection and mitigation components of the MedShield AI framework. The hybrid CNN-LSTM model will be developed using Python and open-source libraries like Scapy and PyShark to capture, filter, and process network packets to analyse traffic patterns and identify potential threats. A lightweight, TinyML-optimised version of the model will be deployed on a prototype gateway, such as a Raspberry Pi, to demonstrate on-device, real-time anomaly detection. This model will be trained to distinguish between benign and malicious network traffic.

5.2 Testing and Quantitative Results

To rigorously test the framework, a dedicated testing environment will be established using publicly available resources.

CICIoMT2024 dataset. This dataset is ideal for this purpose as it contains a variety of attack vectors, including DDoS, DoS, Recon, MQTT, and spoofing, executed against a testbed of 40 real and simulated IoMT devices. The framework's performance will be evaluated against several key quantitative metrics. Our goal is to achieve performance on par with or exceeding that of similar research models, which have demonstrated high accuracy and low false-positive rates.

Our target performance metrics for the on-device intrusion detection system (IDS) are:

- Accuracy: A model similar to ours demonstrated an accuracy of 97.63%, while another achieved 94.87% accuracy with a small implementation budget.
- Precision, Recall, and F1-Score: The system will be benchmarked against these metrics. A comparable model achieved a precision of 0.95, a recall of 0.95, and an F1-score of 0.95, which we aim to match or surpass.
- Response Times: The on-device, edge-based processing is designed to offer low-latency threat detection, which is crucial for real-time applications. Edge computing aims to reduce latency by processing data closer to IoT devices.

5.3 Scalability Analysis

The framework's distributed architecture is inherently designed to overcome the scalability challenges that centralised security models face. By pushing a lightweight threat detection model to the edge/gateway layer, the system can handle a large number of connected devices without overwhelming a central cloud server with raw data traffic. The use of a permissioned blockchain network, such as Hyperledger Fabric, further enhances scalability by enabling efficient governance and data validation among multiple stakeholders without a central authority. This decentralised approach reduces latency and enables cooperation among numerous hospitals, insurance companies, and regulatory bodies as per Figure 7.

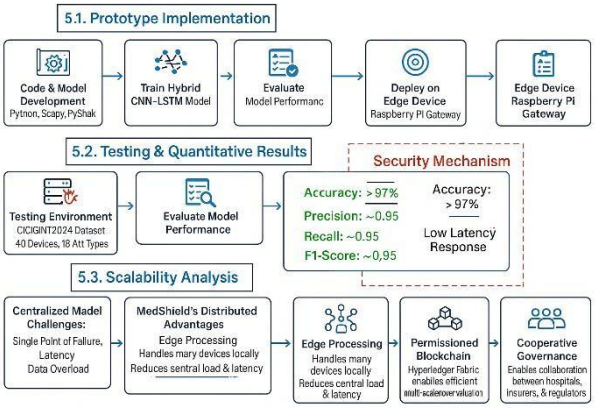

Figure 7: Prototype Implementation, Testing, and Scalability Analysis of the Proposed IoMT Security

6 PRODUCTION-READINESS CHECKLIST FOR IOMT SECURITY FRAMEWORK

This section systematically addresses the critical requirements for transitioning the MedShield AI framework from an R&D project to a production-ready solution.

6.1 Real-World Deployment & Validation

The framework will be tested on a live hospital network in a phased pilot deployment, not just on a simulated dataset. This allows for the evaluation of performance with noisy medical traffic and heterogeneous devices from multiple vendors. A red-team engagement will be conducted to validate the framework's effectiveness against real attack scenarios and exploitation attempts, ensuring its resilience in a high-stakes environment, as per Figure 8.

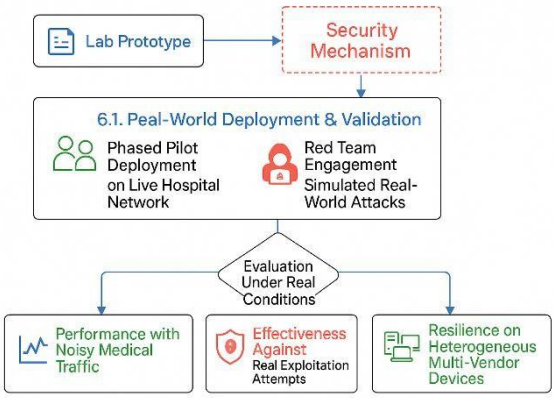

Figure 8: Real-World Deployment and Validation Framework for the Proposed IoMT Security System

6.2 Performance & Resource Optimization

The on-device CNN-LSTM model will be optimised using TinyML techniques to ensure minimal power consumption and a small memory footprint, which is critical for low-power wearables and implantables. We will benchmark latency, throughput, and resource usage to guarantee real-time detection without impacting device performance or battery life. The framework will include a fail-safe fallback mechanism, such as a

rule-based Intrusion Detection System (IDS), which can activate if the ML models fail or are compromised.

6.3 Scalability & Interoperability

To ensure the framework works across multi-vendor ecosystems, it will be designed to support standardised healthcare communication protocols such as HL7, DICOM, and FHIR. The framework will provide a secure API for seamless interoperability and integration with existing hospital IT systems such as Electronic Health Records (EHR) and Picture Archiving and Communication Systems (PACS). Stress testing will be performed to validate the framework's ability to scale for large hospitals with thousands of connected devices, as per Figure 9.

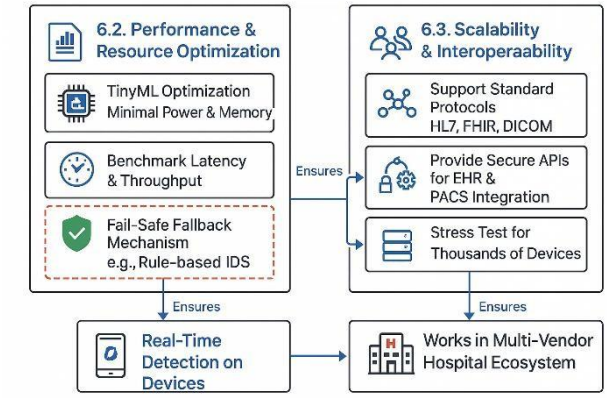

Figure 9: Performance Optimisation, Scalability, and Interoperability Framework for IoMT Security

6.4 Data Privacy & Blockchain Integration

The use of Federated Learning ensures strict GDPR and HIPAA compliance by training the global model on local datasets, ensuring sensitive patient data never leaves its source. The blockchain ledger, a permissioned network using Hyperledger Fabric, will be optimised for low-latency transactions by storing large patient data files off-chain and only anchoring cryptographic hashes on the ledger. This minimises storage overhead while providing an immutable audit trail for all data access and transactions as per Figure 10.

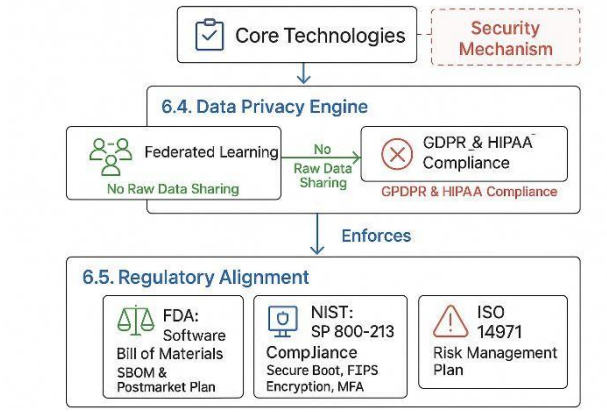

Figure 10: Data Privacy Engine and Regulatory Alignment Framework for Secure IoMT Systems

6.5 Regulatory & Compliance

The research work is fully aligned with regulatory bodies and standards.

- ● FDA: A Software Bill of Materials (SBOM) will be created to demonstrate adherence to FDA premarket and postmarket cybersecurity guidance. A plan for continuous postmarket monitoring and updates will be submitted to the FDA.
- NIST: The framework will be designed to meet the security baseline outlined in NIST SP 800-213, including requirements for secure boot, FIPS 140-2/3 validated encryption for data in transit and at rest, and multi-factor authentication for access control.
- HIPAA & GDPR: Compliance with these data privacy regulations is a core principle of the framework's design, enforced by Federated Learning and the blockchain's access control mechanisms. We will also prepare all necessary compliance documentation, including a risk management plan (ISO 14971), and establish logging mechanisms for legal and forensic purposes.

6.6 Operational Readiness

The project's success hinges on a clear operational plan. This includes developing detailed incident response playbooks for common threats such as ransomware, DoS attacks, and device hijacking. Training programs will be developed for hospital IT and clinical staff to ensure effective use of the framework. We will establish a plan for 24/7 monitoring and integration with existing Security Operations Centres (SOCs). A clear patch and update lifecycle will be established for both the ML models and the blockchain nodes to ensure business continuity even if framework components fail.

6.7 Security Hardening

A comprehensive security hardening strategy will be implemented. This includes enforcing a zero-trust policy at both the device and user levels, and securing all API endpoints with multi-factor authentication and role-based access control. All data, both in transit and at rest, will be protected with FIPS 140-2-validated encryption. The framework will undergo regular threat modelling using frameworks like STRIDE to proactively identify and mitigate new vulnerabilities. The framework is also designed to defend against adversarial machine learning attacks (e.g., poisoned datasets, evasion attacks) by using the blockchain to verify the integrity of shared model updates, preventing malicious actors from compromising the system's intelligence as per Figure 11.

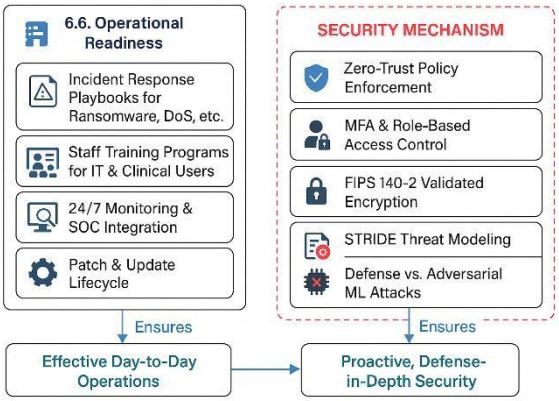

Figure 11: Operational Readiness and Defence-in-Depth Security Framework for IoMT Systems

7 DEPLOYMENT FEASIBILITY AND STANDARDS COMPLIANCE

7.1 Security Standards Mapping

The MedShield AI Framework is designed to align with key healthcare standards, ensuring a clear path to regulatory compliance. The framework's core components are mapped to the requirements of the following standards:

- HIPAA & GDPR: The use of Federated Learning is a foundational component for ensuring compliance with these stringent privacy regulations by enabling collaborative model training without the need to share or centralise sensitive patient data.
- HL7 & FHIR: The framework will support interoperability with existing hospital systems by standardising communication using protocols like Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR).
- ISO/IEC 80001: The framework's design, which emphasises a secure development lifecycle, continuous risk management, and ongoing security testing, aligns with the requirements of ISO/IEC 81001-5-1. These standards mandate the integration of security controls throughout the entire software lifecycle and require regular security audits and penetration testing to identify and mitigate vulnerabilities.

7.2 Cost and Deployment Feasibility

A key consideration for the framework's success is its realistic implementability within a hospital environment. The cost of a comprehensive cybersecurity solution for a hospital can range from $5,000 to $50,000 per month, or between $60,000 and $600,000 per year, depending on factors such as the hospital's size and compliance requirements. While this represents a significant investment, it is a fraction of the financial risk posed by cyberattacks. The average healthcare data breach costs over $1 million, and a single IoMT-related breach can cost as much as $13 million. The MedShield AI framework is designed to be a cost-effective solution by leveraging a hybrid approach that combines an in-house team with outsourced services. Investing in a robust, AI-driven security solution upfront can help hospitals avoid these much larger financial losses and the erosion of patient trust that accompanies a breach.

REFERENCES

[1] Sharma, H., Kumar, P., Shrivastava, G., Sharma, K., & Bhola, A. (2026). Using Machine Learning for Protecting the Security and Privacy of Internet of Medical Things (IoMT) Systems. In *Integrating Cloud, Fog, and Edge Computing in Healthcare: Federated Learning and Blockchain Approaches: Harnessing Distributed Technologies for Enhanced Healthcare Delivery* (pp. 123-138). Cham: Springer Nature Switzerland.

[2] Sharma, H., Kumar, A., & Kumar, G. (2025). Privacy-Enhanced Federated Learning Framework for Intrusion Detection in Smart IoT Environments. *Revolutionary Advances in Computing and Electronics: An International Journal*, 15-25.

[3] Razdan, S., & Sharma, S. (2022). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE technical review*, *39*(4), 775-788.

[4] Dzamesi, L., & Elsayed, N. (2025, April). A review of the security vulnerabilities of the IoMT against malware attacks and DDoS. In *2025, IEEE 4th International Conference on Computing and Machine Intelligence (ICMI)* (pp. 01-08). IEEE.

[5] Deb, S., Lupu, E., Drakakis, E. M., Bharath, A. A., Leung, Z. K., Ma, G. R., & Chattopadhyay, A. (2025). Securing the Internet of Medical Things (IoMT): Real-

World Attack Taxonomy and Practical Security Measures. *arXiv preprint arXiv:2507.19609*.

[6] Morphy, R. (2021). *Fundamental Security for IoT and IoMT Devices within Health Care in the Absence of Industry Standards* (Doctoral dissertation, Capella University).

[7] Al Khatib, I., Shamayleh, A., & Ndiaye, M. (2024, July). Healthcare and the internet of medical things: Applications, trends, key challenges, and proposed resolutions. In *Informatics* (Vol. 11, No. 3, p. 47). MDPI.

[8] Gupta, N., Trivedi, A., Terang, P. P., & Malik, H. (2025). Unveiling Cyber Threats and Digital Forensics. *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*, 35-57.

[9] El-Saleh, A. A., Sheikh, A. M., Albreem, M. A., & Honnurvali, M. S. (2025). The internet of medical things (IoMT): opportunities and challenges. *Wireless networks*, *31*(1), 327-344.

[10] Mohammed, B., Al-Shareeda, M., Hamzah, A., Alhasnawi, B., Homod, R., Alkhabra, Y., ... & Alreshidi, I. (2026). Security challenges and solutions in Internet of Medical Things (IoMT) communication: A review. *Journal of King Saud University Computer and Information Sciences*.

[11] Goel, A., & Neduncheliyan, S. (2024, November). With the convergence of Blockchain, AI, and the Internet of Medical Things (IoMT). In *Machine Learning Algorithms: First International Conference, ICMLA 2024, Himachal Pradesh, India, February 23–24, 2024, Proceedings* (p. 194). Springer Nature.

[12] Alsemmeari, R. A., Dahab, M. Y., Alsulami, A. A., Alturki, B., & Algarni, S. (2023). Resilient security framework using TNN and blockchain for IoMT. *Electronics*, *12*(10), 2252.

[13] Alkatheiri, M. S., & Alghamdi, A. S. (2023). Blockchain-assisted cybersecurity for the Internet of Medical Things in the healthcare industry. *Electronics*, *12*(8), 1801.

[14] Elsayed, N., Dzamesi, L., ElSayed, Z., & Ozer, M. (2025). An extreme learning machine-based system for DDoS attack detection on IoT devices. *arXiv preprint arXiv:2507.05132*.

[15] Shaikh, J. A., Wang, C., Muhammad, W. U. S., Arshad, M., Owais, M., Alnashwan, R. O., ... & Muthanna, M. S. A. (2024). RCLNet: an effective anomaly-based intrusion detection for securing the IoMT system. *Frontiers in Digital Health*, *6*, 1467241.

[16] Faruqui, N., Yousuf, M. A., Whaiduzzaman, M., Azad, A. K. M., Alyami, S. A., Liò, P., ... & Moni, M. A. (2023). SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridisation. *Electronics*, *12*(17), 3541.

[17] Sharma, K. (2022). Internet of healthcare things security vulnerabilities and jamming attack analysis. *Expert Systems*, *39*(3), e12853.

[18] Alalhareth, M., & Hong, S. C. (2024). Enhancing the internet of medical things (IoMT) security with meta-learning: a performance-driven approach for ensemble intrusion detection systems. *Sensors*, *24*(11), 3519.

[19] Choudhury, A., Volmer, L., Martin, F., Fijten, R., Wee, L., Dekker, A., & van Soest, J. (2025). *Advancing privacy-preserving health care analytics and implementation of the Personal Health Train: federated deep learning study. JMIR AI 4: e60847*.

[20] Rahmany, M., & Selvi, A. Ethical and Regulatory Challenges in Securing the Internet of Medical Things (IoMT): A Technical and Policy Perspectives.

[21] Said, A., Yahyaoui, A., & Abdellatif, T. (2023, November). HIPAA and GDPR compliance in IoT healthcare systems. In *International Conference on Model and Data Engineering* (pp. 198-209). Cham: Springer Nature Switzerland.

[22] US Department of Health and Human Services. (2022). Use of online tracking technologies by HIPAA-covered entities and business associates.

[23] Othman, S. B., & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Scientific Reports*, *15*(1), 12358.

[24] 2 Zacharias, C., Jose, J., Zain, M., Noushad, N. M., & Kartha, P. P. (2024, May). Fault Detection using TinyML, Design and Control of Three-Phase Two-Level Inverter. In *2024, IEEE Recent Advances in Intelligent Computational Systems (RAICS)* (pp. 1-6). IEEE.

[25] Elhanashi, A., Dini, P., Saponara, S., & Zheng, Q. (2024). Advancements in TinyML: Applications, limitations, and impact on IoT devices. *Electronics*, *13*(17), 3562.

[26] Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. (2024). Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing IoT device security.

[27] Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. (2024). Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing IoT device security.

[28] Chaudhary, P., Kashyap, V., Sonwal, N., Panwar, P., Dadheech, M., Bhatt, M., & Jain, M. (2023, May). Network Traffic Analysis using Wireshark. In *Geetanjali Institute of Technical Studies* (Vol. 10, No. S2, p. 144).

[29] Poudél, R. (2020). Writing a quick packet sniffer with Python and Scapy.

[30] Dokic, K., Martinovic, M., & Mandusic, D. (2020, September). Inference speed and quantisation of neural networks with TensorFlow Lite for Microcontrollers framework. In *2020, the 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-6). IEEE.

[31] Neil, I. (2024). *CompTIA® Security+® SY0-701 Certification Guide: Master cybersecurity fundamentals and pass the SY0-701 exam on your first attempt*. Packt Publishing Ltd.

[32] Dodge, R. C., Ragsdale, D. J., & Reynolds, C. (2003, October). Organisation and training of a cybersecurity team. In *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483)* (Vol. 5, pp. 4311-4316). IEEE.

[33] Paredes, C., & Ribeiro, P. (2018, September). Future trends in project management. In the *2018 International Conference on Intelligent Systems (IS)* (pp. 637-644). IEEE.

[34] Nalavade, A. V. (2025). AGILE PROJECT MANAGEMENT AND THE FUTURE OF R&D.

[35] Westby, D. M. O. (2018). *DEVELOPMENT OF A PROJECT MANAGEMENT METHODOLOGY FOR CYBER SECURITY ASSESSMENTS* (Doctoral dissertation, UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL).

[36] Neumeier, J., Zelezinskii, A. L., & Arhipova, O. V. (2024). SECURING ENTERPRISES: UNVEILING THE IMPORTANCE AND PROCESS OF PENETRATION TESTING. *Экономический вектор*, (2 (37)), 204-211.

[37] Chu, G., Al-Shareefi, F., Wu, H., Hu, Y., & Yan, S. (2024, December). Penetration Testing for Securing IoT-Enabled Healthcare Systems: A Focus on

Wearable Devices and Remote Surgery. In *2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 5944-5951). IEEE.

[38] Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for medical device cybersecurity in 2018. *Journal of diabetes science and technology*, *12*(4), 743-746.

[39] Rebiere, O., & Rebiere, C. (2017). *Mastering the Gantt Chart: Understand and use the" Gantt Project" open source software efficiently!* (Vol. 1). Rebiere.

[40] Fino, D. F. F. (2025). Leveraging Microsoft Teams for user-focused cybersecurity initiatives and engagement.

[41] Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W. (2018, April). Solution-aware data flow diagrams for security threat modelling, in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing* (pp. 1425-1432).

[42] Workload Management - Industry-Leading Services for Cybersecurity Excellence, accessed September 3, 2025, https://cyberforcerd.com/solutions/workload-management/

[43] Immaculate, S. M. (2026). Chapter 8: Interoperability and Standardisation Challenges in Heterogeneous IoT Environments. *IoT Systems: Architectures, Protocols and Scalable Solutions*, 133.

[44] Kemmerer, R. A. (2003, May). Cybersecurity. In the *25th International Conference on Software Engineering, 2003. Proceedings.* (pp. 705-715). IEEE.

[45] Dover, T. P. (2021). Evaluating medical IoT (MIoT) device security using NISTIR-8228 expectations. *arXiv preprint arXiv:2104.03283*.

[46] Alsubaei, F., Abuhussein, A., & Shiva, S. (2018, October). A framework for ranking IoMT solutions based on measuring security and privacy. In *Proceedings of the Future Technologies Conference* (pp. 205-224). Cham: Springer International Publishing.

[47] Khan, A. A., Laghari, A. A., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alsufyani, H., & Ullah, S. (2025). A lightweight, scalable hybrid authentication framework for Internet of Medical Things (IoMT) using blockchain hyperledger consortium network with edge computing. *Scientific Reports*, *15*(1), 19856.

[48] Sonko, S., Monebi, A. M., Etukudoh, E. A., Osasona, F., Atadoga, A., & Daudu, C. D. (2024). Reviewing the impact of embedded systems in medical devices in the USA. *International Medical Science Research Journal*, *4*(2), 158-169.

[49] Adochiei, F. C., Țoi, F. A., Adochiei, I. R., Argatu, F. C., Serițan, G., & Petroiu, G. G. (2025). HL7 FHIR-Based Open-Source Framework for Real-Time Biomedical Signal Acquisition and IoMT Interoperability. *Applied Sciences*, *15*(23), 12803.

[50] Lechner, N. H. (2017). An overview of cybersecurity regulations and standards for medical device software. In *Central European Conference on Information and Intelligent Systems* (pp. 237-249). Faculty of Organisation and Informatics Varazdin.

[51] Altayyar, S. S. (2020). The essential principles of safety and effectiveness for medical devices and the role of standards. *Medical Devices: Evidence and Research*, 49-55.

[52] Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities*.

[53] Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in the healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73.

[54] Mabina, A., Rafifing, N., Seropola, B., Monageng, T., & Majoo, P. (2024). Challenges in IoMT adoption in healthcare: focus on ethics, security, and privacy. *Journal of Information Systems and Informatics*, *6*(4), 3162-3184.