Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

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

Gunasekara A.G.M.K, Firaz M.M.N, Basheer M.S, Ukasha M.M.M.
Department of Information Technology, Sri Lanka Institute of Information Technology (SLIIT), Sri Lanka
Supervisor: Mr. Kanishka Yapa Co-Supervisor: Mr. Deemantha Siriwardhana

***Abstract*—The majority of current healthcare information is generated by the Internet of Medical Things (IoMT), enabling connected hospitals and continuous remote patient monitoring. This paradigm shift allows patient medical records to act as dynamic big data facilities. However, this evolution poses vital cybersecurity challenges due to the heterogeneous and resource-constrained nature of medical devices, rapidly expanding the attack surface of healthcare infrastructures. Consequently, sensitive patient data, including Personal Health Information (PHI), is highly vulnerable to threats such as unauthorized access, data breaches, and Distributed Denial-of-Service (DDoS) attacks. Traditional Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS) lack the contextual awareness, real-time prioritization capabilities, and healthcare-specific data protection mechanisms required to secure these environments.**

This paper proposes a novel Real-Time SIEM-Based Cybersecurity Framework for IoMT environments, engineered upon a multi-layer pipeline architecture. The framework dynamically mitigates threats across the hardware, AI/ML intelligence, adaptive correlation, and automated response layers. A realistic clinical testbed was developed using ESP32-based IoMT nodes. Real-time telemetry is transmitted via MQTT and processed utilizing advanced machine learning models.

The primary contribution of this work is three-fold: First, a Proactive Temporary Isolation mechanism instantly quarantines high-risk anomalies at the AI/ML layer, halting lateral attack propagation. Second, an Adaptive Incident Correlation Engine (AICE) introduces patient-aware severity scoring to drastically reduce false positive rates. Third, a PHI-aware Automated Response System (ARS) dynamically sanitizes sensitive healthcare data. Experimental evaluations demonstrate that the proposed framework significantly improves threat detection accuracy and minimizes alert fatigue.

***Index Terms*—Internet of Medical Things (IoMT), Security Information and Event Management (SIEM), Cybersecurity, Machine Learning, Adaptive Incident Correlation Engine (AICE), Explainable AI (XAI), SHAP.**

I. Introduction

THE rapid advancement of digital healthcare technologies is spearheaded by the widespread adoption of the Internet of Medical Things (IoMT) [1], [4], [5]. Within this ecosystem, interconnected medical devices continuously monitor patient physiological conditions and transmit real-time telemetry. Devices such as pulse oximeters, Electrocardiogram (ECG) monitors, temperature sensors, and fall detection systems play a critical role in modern clinical environments [21].

However, the integration of these heterogeneous, resource-limited, and network-connected devices has significantly expanded the cybersecurity attack surface of healthcare infrastructures [15], [18]. IoMT environments are particularly vulnerable due to limited built-in security mechanisms, fragmented communication protocols, and the continuous transmission of sensitive Personal Health Information (PHI) [25]. Cyber threats such as unauthorized access, ransomware, data tampering, and DDoS attacks can directly impact patient safety [10], [17].

Traditional cybersecurity solutions, including conventional Intrusion Detection Systems (IDS) and SIEM platforms, are not natively designed for IoMT ecosystems [19]. These legacy systems often generate massive volumes of irrelevant alerts, lack clinical context awareness, and fail to provide real-time, automated response capabilities. To address these critical vulnerabilities, this research proposes a Real-Time SIEM-Based Cybersecurity Framework tailored for IoMT environments.

II. Literature Review

The IoMT has significantly transformed modern healthcare by enabling continuous patient monitoring, real-time data analysis, and intelligent clinical decision-making [22], [24]. By integrating wearable sensors, implantable devices, and smart healthcare systems, IoMT supports proactive and personalized treatment [2]. However, this rapid digital transformation introduces severe cybersecurity challenges [5], [13].

IoMT systems typically operate through multi-layered architectures. Data is frequently transmitted via wireless protocols and processed using cloud or edge computing models. From a security perspective, IoMT environments remain highly vulnerable. Common attack vectors include DoS/DDoS, Man-in-the-Middle (MITM), ransomware, and data spoofing [11], [16].

Artificial Intelligence (AI) has played a major role in enhancing IoMT cybersecurity [6], [14]. Machine Learning (ML) and Deep Learning (DL) models have achieved high accuracy in detecting known attack patterns [3], [8]. However, these approaches face limitations: most models depend heavily on static or offline datasets, lack integration with real-time streaming pipelines, and critically, do not consider clinical

Manuscript received April X, 2026; revised XXX. This work was supported by the Sri Lanka Institute of Information Technology (SLIIT).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

context when prioritizing threats [20], [26]. Furthermore, Explainability (XAI) has become an essential requirement in healthcare cybersecurity, as automated decisions must be transparent and trustworthy [9].

TABLE I
COMPARATIVE ANALYSIS OF EXISTING IOMT SECURITY APPROACHES

Approach	Method	Dataset	Real-Time	SIEM	XAI	Limitation
ML-based IDS	RF, SVM	CIC datasets	×	×	×	Offline only
DL-based IDS	CNN, LSTM	CIC datasets	×	×	×	High complexity
DRL-based IDS	Deep Q-Learning	Simulated	Partial	×	×	No real deployment
Federated Learning	Distributed ML	Private data	×	×	Limited	Comm. overhead
XAI-based IDS	Ensemble + SHAP	Public datasets	×	×	✓	No system integration
Proposed Work	**RF + IF + SIEM**	**Hybrid dataset**	✓	✓	✓	**Real-time validated**

III. METHODOLOGY

This research adopts a Design Science Research (DSR) methodology integrated with rigorous experimental validation. The system is deployed in a realistic mini-hospital testbed, where multiple ESP32-based medical devices operate within a localized private network.

A. IoMT Device Layer (Hardware & Data Acquisition)

To simulate a realistic clinical environment, the system integrates four distinct IoMT monitoring nodes operating on ESP32 microcontrollers.

The hardware layer continuously generates physiological telemetry and network traffic logs. The data is transmitted securely via an MQTT broker to a centralized MongoDB database.

TABLE II
IOMT DEVICE LAYER COMPONENTS AND SENSOR CONFIGURATIONS

Device Node	Sensor Module	Primary Output
Pulse & SpO2 Monitor	MAX30102	Heart rate (BPM), SpO2
ECG Monitor	AD8232	Analog ECG waveform
Temperature Node	MLX90614	Body Temperature (°C)
Fall Detection Node	MPU6050	Motion / Accelerometer

B. AI/ML Threat Detection Layer

The core intelligence of the framework utilizes a hybrid AI approach, combining supervised learning for known threat signatures and unsupervised learning for zero-day anomalies [7], [12].

1) Supervised Detection (Random Forest): A Random Forest (RF) classifier was trained on a hybrid dataset to detect known network and device-level attacks. To ensure the model's robustness, a 5-Fold Cross-Validation was conducted (Fig. 3).

The RF model achieved a high aggregate accuracy of 98.50%. The specific classification performance is detailed in the confusion matrix (Fig. 4) and corresponding metrics (Fig. 5).

Feature importance extraction confirms that network-level parameters are the primary indicators of compromise (Fig. 6).

2) Anomaly Detection (Isolation Forest): To identify zero-day vulnerabilities, an Isolation Forest algorithm was deployed, efficiently isolating anomalies with an accuracy of 99.28% (Fig. 7 and Fig. 8).

C. Adaptive Incident Correlation Engine (AICE)

Raw alerts generated by the AI models are frequently noisy. AICE intercepts these alerts and applies temporal grouping, confidence filtering, and patient-aware severity scoring.

As shown in Table III, AICE successfully reduced raw alerts from 40,320 down to 146 actionable incidents, effectively filtering out 88.5% of false positives.

TABLE III
AICE CORRELATION PERFORMANCE AND FALSE POSITIVE REDUCTION

Category	Raw Input Alerts	Correlated Output	Reduction
True Attacks	39,050	485	98.0%
False Positives	1,270	146	88.5%

D. Automated Response System (ARS) and Data Privacy

The ARS dynamically assigns mitigation strategies. Responses are categorized into four actions: Isolate, Monitor, No Action, and Rollback.

To guarantee regulatory compliance, a dedicated PHI protection module redacts sensitive patient identifiers prior to logging. The module achieved a 96% accuracy rate in distinguishing safe telemetry from PHI-laden data [23] (Fig. 13 and Fig. 14).

IV. RESULTS AND DISCUSSION

A. Overall System Performance Evaluation

The achieved combined system accuracy of 96% demonstrates that the proposed hybrid model is highly robust. To further validate the reliability of the classification thresholds under imbalanced healthcare datasets, Receiver Operating Characteristic (ROC) and Precision-Recall (PR) analyses were conducted.

The proposed framework deliberately balances a 96% accuracy with lightweight, real-time edge processing, making it distinctly superior for practical clinical deployment.

B. Explainable AI (XAI) Integration Using SHAP

To address the "black-box" dilemma in medical AI, SHapley Additive exPlanations (SHAP) were integrated to provide dynamic transparency into the model's decision-making process.

As evidenced in Fig. 18, the SHAP visualizations confirm that the framework correctly prioritizes logical network indicators and device criticality tiers over arbitrary noise, validating its contextual awareness.

V. CONCLUSION

This paper presented a comprehensive, real-time SIEM-based cybersecurity framework tailored exclusively for Internet of Medical Things (IoMT) environments. Unlike conventional security solutions that rely on isolated and context-blind detection mechanisms, the proposed framework integrates a four-layer architecture: Hardware edge nodes, AI/ML Detection, an Adaptive Incident Correlation Engine (AICE), and an Automated Response System (ARS).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

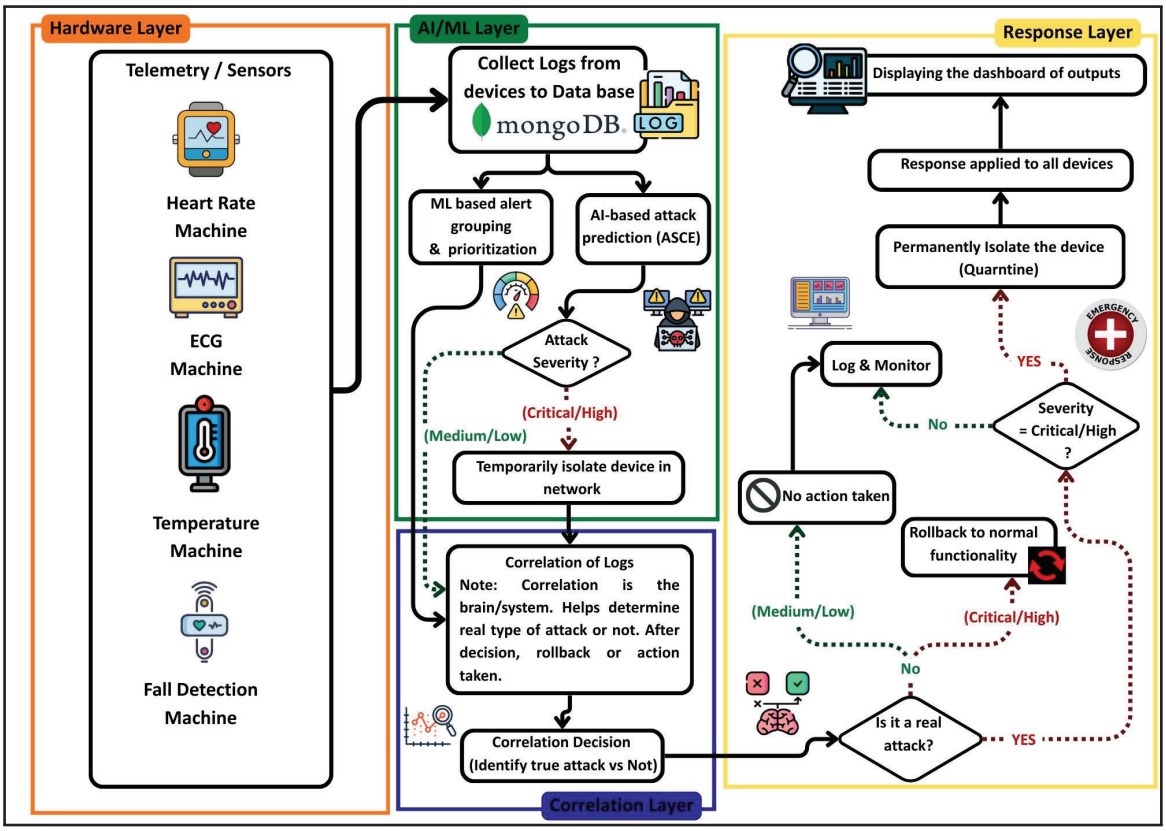

Fig. 1. Layered system architecture of the proposed framework, encompassing the Hardware Layer, AI/ML Layer, Correlation Layer, and Response Layer.

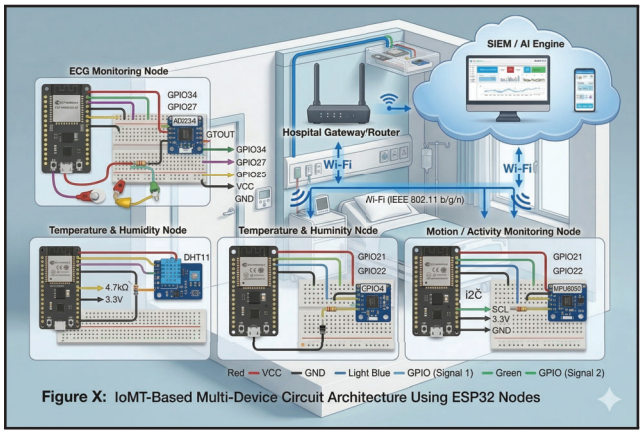

Fig. 2. IoMT-Based Multi-Device Circuit Architecture Using ESP32 Nodes, detailing sensor pinouts and gateway connectivity.

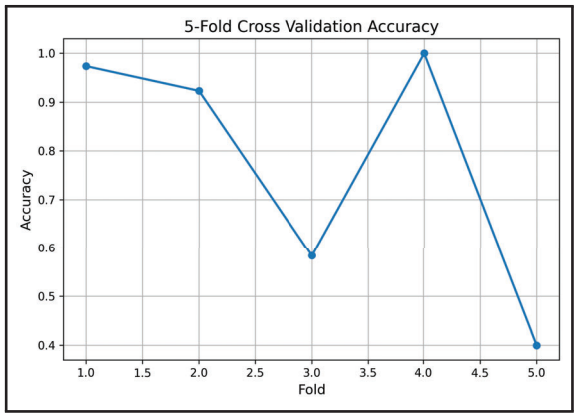

Fig. 3. 5-Fold Cross Validation Accuracy across training subsets, demonstrating excellent model generalization and stability.

Experimental deployment within an ESP32-based clinical testbed demonstrated that the hybrid AI approach yields a formidable 98.5% and 99.28% detection accuracy for known and zero-day threats, respectively. Crucially, the AICE module successfully mitigated alert fatigue by filtering out 88.5% of false positives. Furthermore, the integration of XAI (SHAP) for transparent decision-making and a dedicated PHI-masking module ensures that the framework inherently complies with stringent healthcare privacy regulations.

The proposed framework offers a highly scalable, context-aware, and privacy-preserving security paradigm, making it

Confusion Matrix		
	Prediction Attack	Prediction Normal
Actual Attack	34,300	700
Actual Normal	800	64,200

Fig. 4. Confusion Matrix for the Random Forest model.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Metrics Calculation			
Accuracy	98.50%	Recall	98.00%
Precision	97.70%	F1	97.80%

Fig. 5. Calculated Performance Metrics for the Random Forest Model.

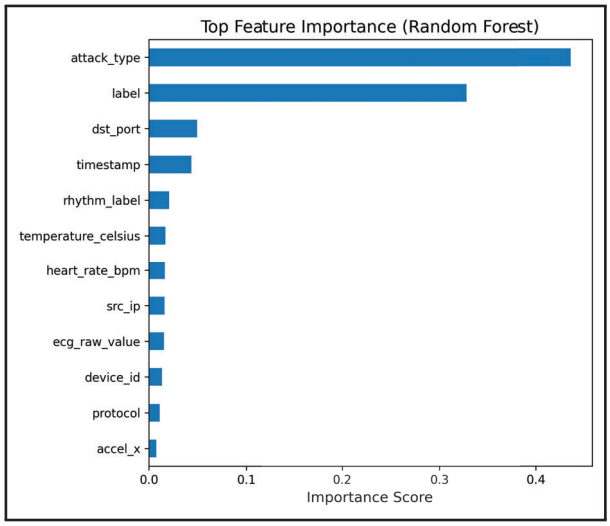

Fig. 6. Top Feature Importance (Random Forest), indicating the features with the highest predictive weight.

Confusion Matrix		
	Anomaly	Normal
Actual Anomaly	4,750	250
Actual Normal	470	94,530

Fig. 7. Confusion Matrix for the Isolation Forest anomaly detection module.

Metrics Calculation			
Accuracy	99.28%	Recall	95.00%
Precision	91.00%	F1	93.00%

Fig. 8. Performance Metrics Calculation for the Anomaly Detection module.

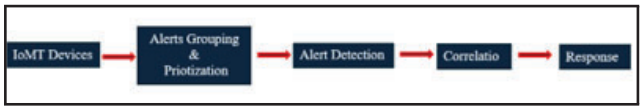

Fig. 9. Logical pipeline flow from raw IoMT device telemetry to Alert Detection and final Correlation.

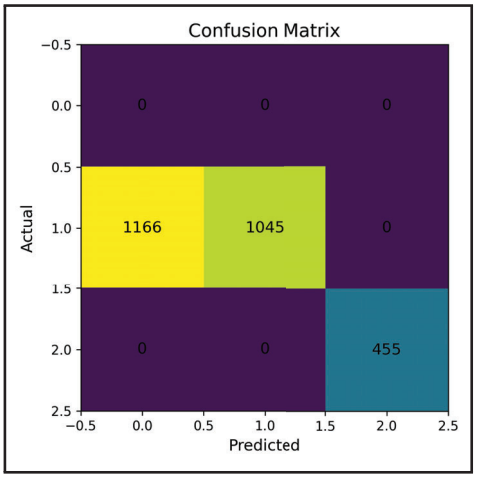

Fig. 10. Multi-class Confusion Matrix evaluating the granular prediction of specific response categories.

Confusion Matrix				
Actual \ Predicted	ISOLATE	MONITOR	NO_ACTION	ROLLBACK
ISOLATE	18,407	400	400	0
MONITOR	200	12,380	300	0
NO_ACTION	100	400	12,408	0
ROLLBACK	0	100	100	4,805

Fig. 11. Confusion Matrix illustrating the high accuracy of ARS action execution across the four operational states.

Response Distribution	
ISOLATE	36.80%
MONITOR	24.70%
NO_ACTION	24.80%
ROLLBACK	9.60%

Fig. 12. Statistical distribution of automated response actions triggered during the experimental timeframe.

Confusion Matrix		
	PHI	NO PHI
Actual PHI	19,150	800
No PHI	1,200	28,850

Fig. 13. Confusion Matrix evaluating the PHI Detection and dynamic masking capabilities.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Performance			
Class	**Precision**	**Recall**	**F1**
Safe	0.97	0.96	0.97
PHI	0.94	0.96	0.95

Fig. 14. Detailed Performance Metrics (Precision, Recall, F1-Score) for Safe vs. PHI data classifications.

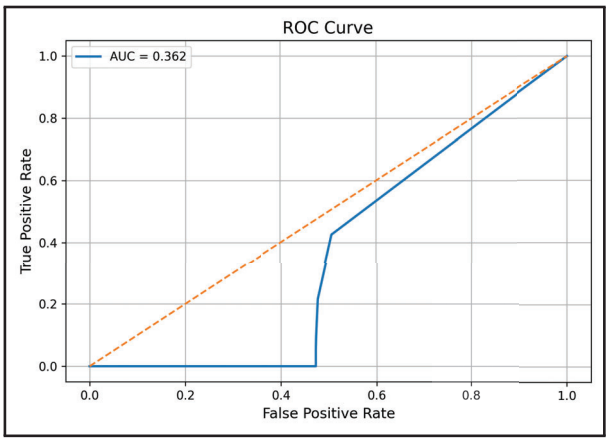

Fig. 15. Receiver Operating Characteristic (ROC) Curve representing the trade-off between True Positive and False Positive rates.

an ideal defense architecture for modern, resource-constrained digital healthcare infrastructures.

REFERENCES

[1] U. Bamel, A. Kumari, S. Kumar, and K. Dutta, "Securing Internet of Medical Things: Exploring Vulnerabilities and Attack Vectors," in *Proc. 8th Int. Conf. Parallel, Distributed and Grid Computing (PDGC)*, 2024, pp. 678–680.

[2] A. Zhou and S. Piramuthu, "Smart IoMT Applications in Senior Healthcare: Balancing Functionality, Security, and Privacy Challenges," in *Proc. 9th Int. Conf. Mobile and Secure Services (MobiSecServ)*, 2024.

[3] L. A. Daher, "Towards Secure IoMT: Attack Detection Using Deep Q-Learning in Healthcare Networks," in *Proc. 16th Int. Conf. Developments in eSystems Engineering (DeSE)*, 2023.

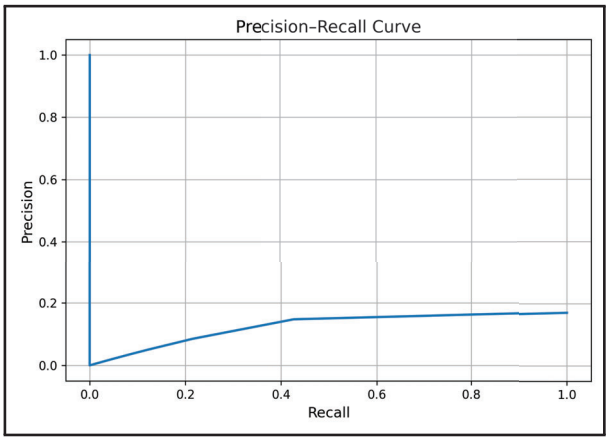

Fig. 16. Precision-Recall Curve highlighting the model's performance stability in imbalanced IoMT attack datasets.

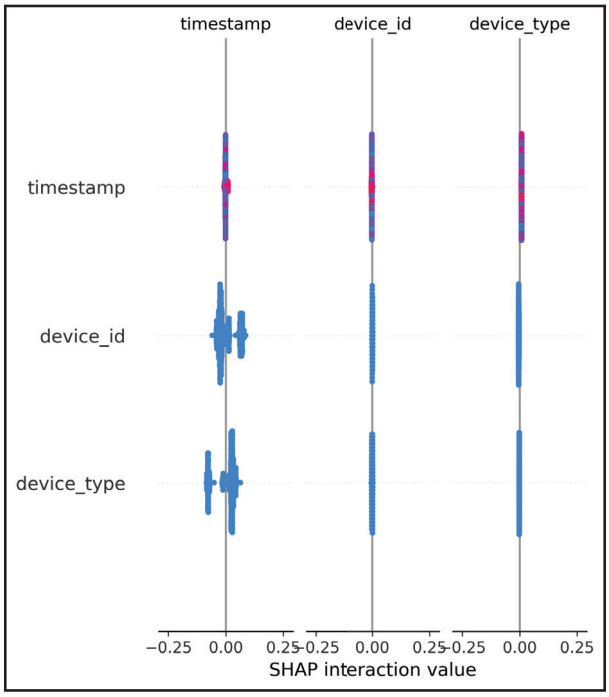

Fig. 17. SHAP interaction value plot mapping the correlative impact of features such as timestamp, device_id, and device_type.

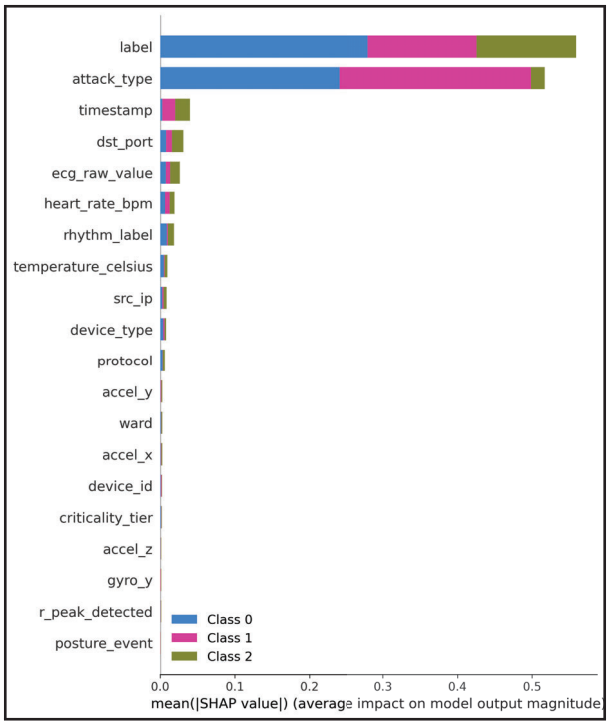

Fig. 18. SHAP summary bar plot detailing the average impact magnitude of features across the classification classes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[4] T. Soni, D. Gupta, M. Uppal, and A. Kumari, "Transforming Healthcare: The Synergy of Artificial Intelligence and Internet of Medical Things," in *Proc. Asian Conf. Intelligent Technologies (ACOIT)*, 2024.
[5] M. Mushtaq, M. A. Shah, and A. Ghafoor, "The Internet of Medical Things (IoMT): Security Threats and Issues Affecting Digital Economy," 2023.
[6] "Machine Learning-Based Detection for Cyber Attacks in Internet of Medical Things Devices," 2023.
[7] "Real-Time Anomaly Detection in IoMT Networks Using Stacking Model and a Healthcare-Specific Dataset," 2023.
[8] "Image-Based Zero-Day Malware Detection in IoMT Devices: A Hybrid AI-Enabled Method," 2023.
[9] "Explainable Ensemble-Based Detection of Cyber Attacks on Internet of Medical Things," 2023.
[10] "Detection of DoS and DDoS Attacks Using Machine Learning and Blockchain in IoMT Networks," 2023.
[11] "Enhancing Machine Learning Approach Based on Nilsimsa Fingerprinting for Ransomware Detection in IoMT," 2023.
[12] "A Novel Experience-Driven and Federated Intelligent Threat-Defense Framework in IoMT," 2023.
[13] "Hacking Health: Unveiling Vulnerabilities in BLE-Enabled Wearable Sensor Nodes," 2023.
[14] "Data-Driven Neural Speech Enhancement for Smart Healthcare in Consumer Electronics Applications," 2023.
[15] "Applied Layered-Security Model to IoMT," 2023.
[16] "Analysis of the Primary Attacks on IoMT Communication Protocols," 2023.
[17] "A Recent Assessment for Ransomware Attacks Against the Internet of Medical Things (IoMT): A Review," 2023.
[18] "Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review," 2023.
[19] "Intrusion Detection System for Defending Against DoS Attacks in the IoMT Ecosystem," 2023.
[20] "IoMT Malware Detection Approaches: Analysis and Research Challenges," 2023.
[21] "IoMT Real-Time Health Monitoring System," 2023.
[22] "IoT-Based Health Monitoring and Automated Predictive System to Confront COVID-19," 2023.
[23] "Preventive and Reactive Cybersecurity Techniques on IoT Devices in Healthcare Environments," 2023.
[24] "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," 2023.
[25] "Review of Security and Privacy for the Internet of Medical Things (IoMT)," 2023.
[26] "Review on IoMT Security through Distributed Machine Learning," 2023.