MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3457-3460

CYBER THREAT HUNTING IN IOMT; ENHANCING SECURITY THROUGH PROACTIVE DETECTION

MS .JAYASHREE S, ASSISTANT PROFESSOR, jayashree.s@kgkite.ac.in Department of Computer science and Engineering, KGISL Institute of Technology, Coimbatore, India.
MANOJ KUMAR R manojr24062005@gmail.com, NITHIESH S selvarajs7107@gmail.com, VISHWA A J 1vishwa.v.j.dae4@gmail.com Department of Computer science and Engineering, KGISL Institute of Technology, Coimbatore, India.

Abstract
the Internet of medical things (IoMT) is far too common in the medical field, in the exchange of medical information among the interconnected devices.this can be convenient in continuous check on the patients, it is also therat to security. This paper will highlight the number of cyber threats encountered through the utilization of the traditional security systems, which reacts once an attack has occurred.This paper shall focus on the early identification of cyber threats in the IoMT networks using a machine learning-based approach. The suggested system monitors the traffic and trains the network in which the IoMT devices will interact with each other. A possible indicator of an barred act is the abnormal or unpredictable presence in the stream of the data. This will facilitate in detecting both the known and unknown attacks before they can create severe destuction upon the network.The system will be in a position to verify the activity going on the internet and isolate the normal and potential activity providing quick response as well as enhanced security awareness. The primary idea of this work is how the safety and reliability of the IoMT-based healthcare systems can be enhanced through the suggestion of the proactive approach to their detection.
Keywords—IoMT, Cybersecurity, Network Monitoring, Anomaly Detection, MachineLearning, Proactive Threat Detection,Healthcare Systems

I. INTRODUCTION

Over the past few years, the healthcare sector has highly adopted the Internet of Medical Things (IoMT) to support patient monitoring, diagnosis, and treatment. medical devices such as wearables, infusion pumps, and monitoring systems continuously exchange data among hospital and cloud networks,third party services. While this connectivity improves healthcare efficiency, it has also increased the exposure of medical systems to cyber threats. Even a small security threat can quickly leads into a serious incident, affecting patient safety, data privacy, and system availability. Cyberattacks on healthcare systems can have consequences apart from data loss. Unauthorized access or manipulation of medical data may lead to incorrect health care decisions and loss of trust in healthcare institutions. In addition, malware attacks can collapse hospital operations, resulting in financial losses and delays in patient care. Due to the sensitive nature of medical information, IoMT networks have become attractive targets for attackers.

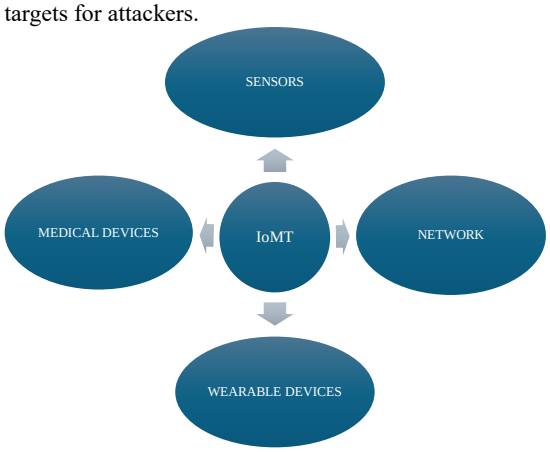

Fig1:blocks of iomt

Eventhough advancements in cybersecurity, many existing security mechanisms used in healthcare environments still works in a reactive approach. Traditional intrusion detection systems and rule-based monitoring tools often rely on known attack signatures and predefined thresholds. As a result, new or hidden attacks may become undetected for long periods, while dynamic network conditions can lead to false alarms or missed threats. The increasing availability of network data from IoMT systems creates an opportunity for more intelligent security solutions. Machine learning techniques can analyze large volumes of network traffic, learn normal communication behavior, and identify subtle deviations that may indicate malicious activity. With this motivation, this work focuses on proactive cyber threat hunting in IoMT networks using machine learning. The proposed approach aims to detect potential threats at an early stage, improve security visibility, and enhance the overall reliability of connected healthcare systems.

II. LITERATURE REVIEW:

A. Security Problems in IoMT Environment:

Internet of Medical Things (IoMT) has demonstrated to be a meaningful phenomenon with a positive impact on healthcare, yet, it has triggered severe cybersecurity risks. The security of IoMT devices is also relatively weak, and they are easily attacked, interfering with patient data and interrupting vital services. According to recent surveys in the area of IoMT security, attackers are capitalizing on communication vulnerabilities, inadequate authentication, and device resource constraints that have challenges in mitigating threats using the conventional security mechanisms [20], [21]. Also, the importance of specifically designed cerebrated intrusion detection systems in IoMT environments is also suggested by detailed reviews since the standard methods to ensure IoT security cannot be adapted to healthcare-specific threat trends and regulatory needs [16], [17].

B. AI-based and Network-based Threat Detection:

To enhance threat detection on IoMT networks, a number of researchers have paid attention to network traffic analysis to identify anomalies in network traffic instead of depending on signature-based techniques [23]. It has proposed advanced methods of intrusion detection that is based on AI and caters to dynamic and emerging threats [13]. As an illustration, a more advanced intrusion detection approach employs the probabilistic neural networks and optimization algorithms to ensure communication between IoMT devices, which proves to be more effective in detection of intrusion compared to classical approaches [2]. Other articles take advantage of ensemble and deep learning techniques to make attack detection more resilient, and it has been demonstrated to be more successful by the use of better feature extraction and imbalance management strategies [7], [19].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3423-3426

C. Machine Learning and Deep Learning Techniques of Threat Hunting in IoMT:

The recent works also combine models of machine learning and deep learning to identify the intricate attack patterns in the internet of things [5], [6]. A hybrid network of Graph Convolutional Networks (GCN) and transformer networks demonstrated that the ability to distill both relational and sequence patterns of real IoMT traffic can be used to improve the performance of early threat detection [12], [3]. In another study, an intrusion detection system called anomaly-based intrusion detection system (RCLNet) was introduced, and it is based on CNN and LSTM models in combination with adaptive mechanisms to deliver high accuracy on healthcare data, surpassing traditional intrusion system methods [4], [11]. Also, models of reinforcement learning-based IDS have been suggested, which allow making dynamic decisions and responding better to new network threats [9], [14].

III. PROBLEM STATEMENT

Despite the range of security solutions that have been proposed to the Internet of Medical Things (IoMT), the biggest portion of those solutions are reactive-based solutions, which disclose a threat once it has been executed by an intruder user. More advanced or covert threats that may be found within the normal network traffic will not be identified by conventional signature detectors and basic anomaly detectors. As a result, the confidential attacks of the IoMT networks may remain uninformed over a considerable period of time, jeopardizing sensitive patient information, and jeopardizing the healthcare services. Some of the solutions available also have constraints of implementation. The machine learning models that are built on large labeled data sets are not easily trained in real medical practice due to privacy and the inability to get exhaustive information about attacks. This limits their functionality in real IoMT systems. The other techniques are too computer-intensive to perform threat detection in real time, so real-time threat detection cannot be done on scale and constantly moving network traffic.Other than that, most of the systems that are already in place have not adequately integrated their continuous network monitoring, intelligent threat analysis and timely alerting needed to respond and mitigate as quickly as possible. The challenge of these issues is that an adaptive, active, and lightweight machine learning-based threat hunting framework on IoMT is needed to address these problems and learn the normal behavior of the network relentlessly to identify slight contravention of the norm that may point to malicious intent. This will assist in the early and reliable detection of known and unknown attacks and improve the overall security and the dependability of the IoMT-based healthcare systems.

IV. METHODOLOGY

This system follows a step-by-step process combining IoMT network monitoring and machine learning to detect cyber threats earlier. It continuously collects network traffic data, preprocesses it, extracts important features, and uses a machine learning model to identify anomalous behavior. Based on the model's output, the system generates real-time alerts, helping to detect cyber-attacks before they compromise patient safety or data integrity.

Data Acquisition: The system continuously monitors IoMT network traffic, collecting information from medical devices, sensors, and gateways. Critical data includes device communication patterns, protocol usage, connection frequency, and packet characteristics, which are essential for assessing network security risks.

Hardware and Network Components: IoMT Devices: Wearables, monitors, and medical sensors transmitting patient data.
Edge Gateway: Aggregates data from multiple devices and forwards it securely to the processing module.
Monitoring Server: Receives and stores network traffic for feature extraction and anomaly detection.

Data Preprocessing: Raw network traffic may contain noise, missing values, or irrelevant packets. Preprocessing ensures clean and consistent data for model training:

1. Data Cleaning: Corrects missing or corrupted data points.
2. Outlier Removal: Filters spikes caused by network glitches to prevent false alerts.
3. Normalization and Encoding: Scales and converts features into formats suitable for machine learning models.

Feature Extraction

1. The system derives key indicators of abnormal network behavior:
2. Traffic Change Rate: Detects sudden spikes in device communication.
3. Connection Count: Tracks unusual increases in simultaneous connections.
4. Protocol Patterns: Identifies deviations from normal protocol usage.
5. Composite Feature Vector: Combines multiple indicators into a single input for the model.

These features help the model detect subtle anomalies that traditional signature-based approaches might miss.

Model Development: The system uses unsupervised machine learning to learn normal network behavior and detect deviations:
Isolation Forest Algorithm: Identifies unusual patterns in the network without requiring labeled attack data.
Anomaly Scoring: Each network instance is scored based on deviation from normal behavior. Higher scores indicate higher risk.
Model Training: Uses historical normal network traffic data to train the model efficiently.
Comparative models such as Autoencoders, SVMs, and Random Forests were also evaluated, but Isolation Forest proved superior in accuracy, speed, and low resource requirements.

Model Evaluation: The model's effectiveness is measured using:

1. Precision: Ability to correctly detect malicious events.
2. Recall: Ability to detect all potential threats.
3. F1-Score: Overall balance of precision and recall.
4. Latency: Average prediction time per network instance.

The Isolation Forest achieved high accuracy and low latency, suitable for real-time monitoring in IoMT networks.
Prediction and Alert System
Once trained, the model is integrated with the live network stream to provide continuous anomaly detection:

1. Safe: Normal network behavior.
2. Warning: Suspicious activity detected.
3. Alert: High chance of cyber-attack.

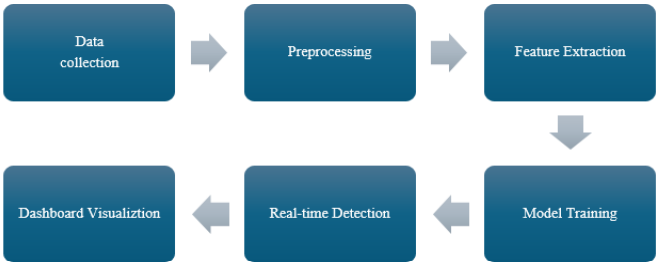

Fig 2: Workflow diagram

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3423-3426

Alert Workflow:
Anomaly Detected → Score exceeds threshold.
Event Logging → Timestamp and network details recorded.
Dashboard Update → Security team sees real-time alerts and network status.
Notifications → Automated alerts sent to administrators for immediate action.
This setup enables proactive detection, quick response, and enhanced security for IoMT devices and patient data.

V. IMPLEMENTION:

The proposed system implementation is aimed at the monitoring of real-time, anomaly detection, and proactive mitigation of threats in the networks of internet of things, IoMT. The system is also developed to repeatedly keep track of network data flow of medical equipment like wearables, patient monitors, infusion pumps, and intelligent sensors without any interruption to their usual functionality. The entire traffic of the devices is collected using an edge gateway that does minimal processing and then sends the information to a central monitoring server to be analyzed further. The strategy guarantees low latency, less network congestion, and enhanced responsive time to possible threats.

After the network traffic has arrived at the monitoring server it is preprocessed to present clean and consistent data. Raw network data frequently includes noise, missing values, or uninteresting packets and therefore preprocessing can involve clean up of corrupted entries, the removal of temporary spikes due to network glitches, the normalization of the numerical features and the encoding of categorical values. Traffic is also pooled on specific time periods so as to determine trends and abrupt deviations effectively. Several important features that depict a normal and an abnormal device behavior are then extracted using this clean and structured information. Significant signs also are traffic surges, abnormal number of connections, protocol deviation, and device-specific traffic patterns. These characteristics enable the system to identify minor anomalies, which traditional threshold methods may fail to identify.

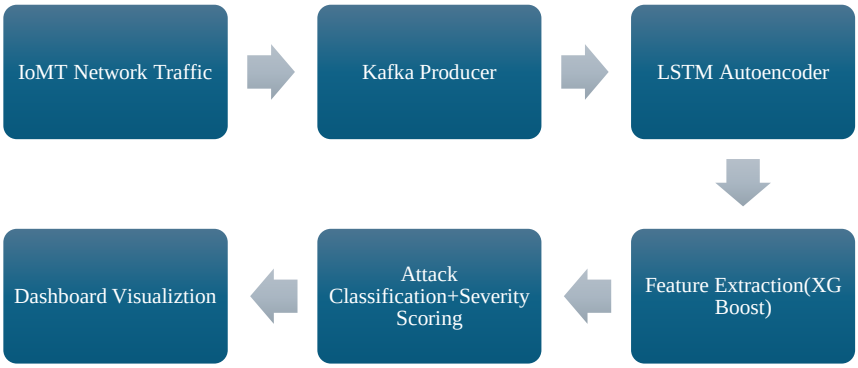

Fig 3: System architecture diagram

The Matthias Forest machine learning model is at the center of the system and the model is unsupervised. The model gets to learn the normal behavior of the IoMT devices during the training phase based on historical traffic information. Being constantly up to date in a live state, the model analyzes current traffic and provides anomaly scores to point out unusual behavior. In contrast to supervised learning models, the Isolation Forest does not need labeled data of attacks, which is especially valuable when the latter is not available in healthcare networks. Similar analyses to other models such as Autoencoders, SVM, and Random Forests demonstrated that the Isolation Forest offered the most combination of accuracy, efficiency as well as minimal resource usage thereby being ideal in resource-scarce IoMT settings. Identified anomalies are transformed to explainable alerts to administrators: Safe, Warning or Alert. Alerts can be centralized in a database and shown on a real time dashboard, enabling the security personnel to watch numerous devices at the same time, trends over time, and which actions to take in response priority. It is also possible to send notifications automatically using email or messaging because it is necessary to focus on a situation immediately.

Layer	Component	Technology
Data Streaming Layer	IoMT Network Traffic + Kafka Producer & Broker	Apache Kafka (kafka-python), Docker
Processing Layer	IoMT Network Traffic + Kafka Producer & Broker	Python, Pandas, NumPy
Anomaly Detection Layer	LSTM Autoencoder (Reconstruction Error Detection)	TensorFlow / Keras
Classification Layer	Attack Classification (XGBoost / Random Forest)	Scikit-learn, XGBoost
Visualization Layer	Real-Time Dashboard & Alerts	Streamlit, CSV Logging

Table 1:Layer Architecture Table

To measure the performance of the system, a simulated and real IoMT network traffic have been used. The test showed that the detection was very high, the false positive was very low and the latency was low providing real time detection of anomaly. Scalability was also ensured and the system was able to support several devices at a time without affecting its performance. A number of deployment concerns were also considered such as ensuring privacy of patient data, keeping the computation load to a minimum to not interfere with the work of medical equipment, the variety of device types and protocols and a flexible alert system that would minimize alert fatigue among administrators. In general, the execution presents a vigorous, lightweight and dependable IoMT security system. The system provides early warnings on cyber threats by combining continual network monitoring services, advanced features extraction, and unsupervised anomaly detection, safeguarding the patient information and integrity of the related medical devices. Its scalable and modular architecture gives it an easy time integrating with larger IoMT networks, which is why it is suitable to the present-day healthcare setting.

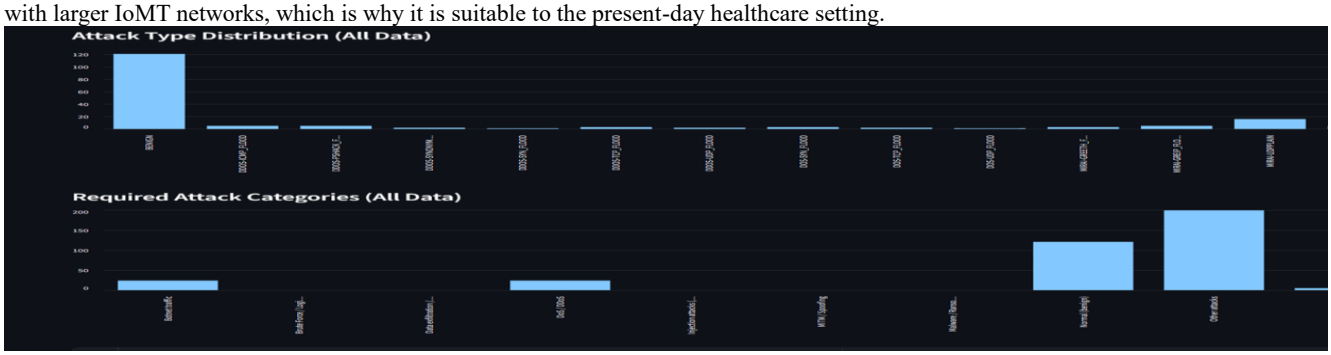

Fig 4: Attack type distribution

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3423-3426

VI. CONCLUSION

In the paper, we suggested a proactive IoMT cyber threat hunting system, a combination of real-time network monitoring, sophisticated feature extraction, and unsupervised machine learning to detect anomalies. In contrast to the classical reactive security systems, the proposed system is used to continuously monitor the behavior of the device, identify even the slightest deviation from the regular patterns and give timely alerts to the administrators through a well-developed dashboard. The strategy aims to make sure that the possible cyber threats can be identified before having the power to breach patient records or disrupt the operations of a healthcare system, thereby contributing to the overall effectiveness and safety of the healthcare networks.

It was shown that the Isolation Forest algorithm can be deployed successfully to IoMT settings, providing high detection rates, low latency, and low computational cost, which is appropriate to deploy in real-time in systems with limited resources. The modular and scalable architecture, in addition, enables the integrative utility with diverse IoMT equipment, which is feasible in the current healthcare systems.

On the whole, this paper suggests the significance of proactive threat detection in IoMT networks, as it demonstrates that the integration of the IoT data collection with smart anomaly detection can lead to the essential enhancement of cybersecurity without affecting the performance of devices. The future of work can be aimed at implementing various machine learning models, improving predictive features, and decreasing the scope of the system to large-scale hospital networks consisting of heterogeneous IoMT devices.

VII. FUTURE ENHANCEMENT:

- The proposed system provides a solid foundation for IoMT cyber threat detection, and several enhancements can further improve its performance and scalability. Integration of advanced models such as **Transformer-based architectures** can improve temporal pattern learning compared to LSTM. Incorporating **Isolation Forest or hybrid anomaly detection techniques** can enhance the detection of unknown and zero-day attacks.
- The system can be extended to support **real-time alert mechanisms** such as SMS, email, or mobile notifications for faster incident response. Deployment on **cloud platforms** (AWS, Azure) will enable large-scale monitoring of distributed healthcare networks. Additionally, integrating **Graph Neural Networks (GNNs)** can help analyze device-to-device communication patterns for detecting complex attacks like botnets.
- Further improvements include adding **automated response systems** (e.g., blocking suspicious IPs), enhancing data preprocessing for better accuracy, and supporting **multi-source data inputs** such as logs and sensor data. These enhancements will transform the system into a **fully autonomous and enterprise-grade IoMT security solution**.

VII. REFERENCES

[1] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, “Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation, and ML Evaluation,” IEEE Access, 2025.
[2] M. Alalhareth and S.-C. Hong, “An Adaptive Intrusion Detection System in the Internet of Medical Things using Fuzzy-Based Learning,” Sensors, vol. 23, no. 22, 2023.
[3] M. Z. Khan, A. Sabur, and H. Ghandorh, “A Novel IoMT Hybrid Model for Cybersecurity Anomaly Detection,” Sensors, vol. 25, 2025.
[4] J. A. Shaikh et al., “RCLNet: An Effective Anomaly-Based Intrusion Detection for Securing the IoMT System,” Frontiers in Digital Health, vol. 6, 2024.
[5] S. Rathore and J. H. Park, “Anomaly Detection in IoT Healthcare Systems using Machine Learning and Cloud-Edge Architecture,” IEEE Access, vol. 11, 2023.
[6] H. Sedjelmaci and S. M. Senouci, “Machine Learning-Based Anomaly Detection for IoT Healthcare Systems,” Computer Networks, vol. 230, 2023.
[7] K. S. Hossain et al., “Hybrid Anomaly Detection Model for IoMT Security using Ensemble Learning,” IEEE Access, vol. 12, 2024.
[8] M. Alrashdi and S. Alqahtani, “Edge-Based Anomaly Detection for Secure IoMT Communications,” Future Internet, vol. 16, 2024.
[9] A. Ullah et al., “Federated Learning-Based Intrusion Detection for IoMT Environments,” Future Internet, vol. 16, 2024.
[10] T. D. Nguyen et al., “Lightweight Intrusion Detection Framework for IoT-Based Healthcare Networks,” Sensors, vol. 24, 2024.
[11] L2D2: A Novel LSTM Model for Multi-Class Intrusion Detection Systems in IoMT (IEEE Access, 2025).
[12] Transformer-Based Intrusion Detection for Securing Medical Applications in 5G IoMT Networks, IEEE CS BDC Symposium, 2024.
[13] A. Alrubayyi, M. S. Alshareef, Z. Nadeem, A. M. Abdelmoniem, and M. Jaber, “Security Threats and Promising Solutions Arising from the Intersection of AI and IoT,” Future Internet, vol. 16, no. 3, 2024.
[14] Intrusion Detection in IoT leveraged by Multi-Access Edge Computing using Machine Learning, IEEE Conference Publication, 2025.
[15] IoT Security: A Deep Learning-Based Approach for Intrusion Detection and Prevention, IEEE Conference Publication.
[16] M. Usman et al., “A Survey on Intrusion Detection in IoT Healthcare Systems using Machine Learning Techniques,” IEEE Access, vol. 11, 2023.
[17] A. Arshad, F. Aadil, and A. Azam, “A Survey: Machine Learning Approaches and Intrusion Detection Techniques for IoT,” IEEE Access, vol. 8, 2020.
[18] H. Alrubayyi et al., “AI-Driven IoT Security: Review of IDS, Datasets, and Cloud-Fog-Edge Architectures,” IEEE IoT Journal (accessible open portions).
[19] “Machine Learning-Based Detection of IoT Network Anomalies,” IEEE Security & Privacy (ensemble autoencoder methods, open access edition).
[20] A. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” IEEE Access, vol. 7, 2019.
[21] K. Zhao and L. Ge, “A Survey on the Internet of Things Security,” IEEE Computational Intelligence & Security Conference, 2023 (open proceedings).
[22] O. Bello and S. Zeadally, “Intelligent Device-to-Device Communication in IoT,” IEEE Systems Journal, vol. 11, 2017 — fundamental IoT security concepts.
[23] Y. Xiao, D. K. Yau, and K. Chen, “Proactive Network Monitoring and Threat Detection for IoT Systems,” IEEE Trans. on Info. Forensics & Security, 2020.
[24] Enhancing IoT Security: A Machine Learning Approach to IDS Evaluation, IEEE Conference, 2025 — network-based ML evaluation.
[25] Anomaly-Based Intrusion Detection for IoMT: Design & Evaluation, IEEE Access, 2025 (expanded open access evaluation)