International Journal of Innovative Research in Engineering
Volume 7, Issue 2 (March - April 2026), PP: 109-115.
https://www.doi.org/10.59256/ijire.20260702015
www.theijire.com
ISSN No: 2582-8746

Cyber security Risk Assessment in Medical IoT (MIoT) Networks

Balakshaj B[1], Balaji Sai Y[2], Dr. J. Refonaa[3]
[1,2,3] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology Chennai, Tamil Nadu, India.

How to cite this paper:
Balakshaj B[1], Balaji Sai Y[2], Dr. J. Refonaa[3], Cyber security Risk Assessment in Medical IoT (MIoT) Networks", IJIRE-V7I2-109-115.

Abstract: *The intensive implementation of Medical Internet of Things tools has enhanced the efficiency of patient monitoring but has also exposed the system to more cyber threats likely to compromise data integrity and reliability of the devices. The given paper introduces a real time cybersecurity monitoring system, which is developed according to a simulated medical IoT environment. The architecture consists of data simulation, anomaly detection, and rule based risk assessment integrated into an interactive monitoring dashboard proposed. It is completely implemented in Python and Streamlit, and it allows seeing the behavior of the devices without using external storage systems. Artificial medical device data in terms of heart rate, temperature, blood pressure and battery condition is produced to simulate normal and attack conditions. The abnormal behavioral patterns are detected in real-time with the help of a machine learning model that is based on unsupervised anomaly detection. Simultaneously, a rule based engine tests various security conditions such as abnormal vital range, validation of device identity, consistency of timestamps and reliability of signals. To enhance its interpretability and reliability, outputs of both the detection layers are used to generate alerts. The dashboard has real time charts, alerts and mitigation recommendations like device blocking or quarantine. The system shows the effectiveness of hybrid-based methods in an effective medical IoT security monitoring interface. The present work illuminates that it is possible to apply lightweight analytics and visualization tools to enable proactive cyber risk awareness in healthcare-linked devices.*

Keywords: *Artificial Intelligence, Natural Language Processing, Legal Document Analysis, Transformers, Hybrid Summarization, Clause Extraction, Machine Learning Classification, Multilingual Support.*

I.INTRODUCTION

The Medical Internet of Things has become an important part of modern healthcare systems by enabling continuous monitoring of patient vital signs through connected devices. Wearable and bedside medical sensors such as heart rate monitors generate a constant stream of data that supports timely clinical decisions. While these devices improve healthcare efficiency, they also introduce new cybersecurity risks. Medical IoT devices often operate continuously, rely on wireless communication, and function with limited computing resources, which makes them attractive targets for cyber- a ttacks. Any disruption ormanipulation of medical data can directly affect patient safety and trust in healthcare systems.

Traditional security mechanisms are often not sufficient for Medical IoT environments because they are designed for static networks and well defined attack patterns. Medical devices generate dynamic data streams, and abnormal behavior may occur due to both malicious activity and natural system variations. This creates a need for continuous monitoring systems that can detect unusual behavior in real time and provide understandable alerts to system operators. Lightweight detection approaches are especially important, as medical devices cannot support heavy security processing.

This project focuses on the design and implementation of a real time cybersecurity monitoring system for a simulated Medical IoT device. The system is developed entirely in Python and uses an interactive dashboard to visualize device behavior as it occurs. Instead of relying on external datasets or stored logs, the system generates synthetic device data in real time. This approach allows controlled evaluation of both normal operation and attack conditions within a single environment. The simulated data includes key parameters such as heart rate, temperature, blood pressure, battery level, and device identity information.

To improve detection reliability, the system adopts a hybrid approach that combines machine learning based anomaly detection with rule based risk assessment. An unsupervised learning model is used to identify deviations from normal patterns in selected device parameters. This enables the system to detect previously unseen or irregular

behavior without requiring labeled training data. Alongside this, a rule based engine evaluates predefined security conditions that reflect common operational and integrity issues in medical devices. These rules check for abnormal vital ranges, low battery conditions, identity inconsistencies, timing errors, and signal related faults.

The outputs from both detection layers are integrated within a single monitoring interface. The dashboard displays real time charts, alert messages, and system statistics such as detected anomalies and uptime. It also includes basic mitigation controls that allow the user to simulate actions such as device blocking or quarantine. By presenting security information in a clear and interpretable manner, the system supports informed decision making during abnormal events.

This work demonstrates a practical approach to Medical IoT security monitoring using lightweight analytics and visualization techniques. The implementation highlights how hybrid detection strategies can be applied within an operational dashboard to enhance cyber awareness and improve the resilience of connected healthcare devices.

II.LITERATURE SURVEY

The use of Medical Internet of Things devices is increasingly affecting healthcare monitoring and the delivery of services greatly. Nevertheless, sensing, communication, and computation integration in the medical setting have posed significant cybersecurity issues as well. In the recent past, research has been done on the concept of security risks, detection methods and the development of structures to be used in the hybrid systems to safeguard sensitive medical information and device operation.

Ali et al. refer to the current trends and security issues in healthcare IoT systems and state that medical devices are vulnerable to cyber attacks because of the constant connection and the lack of computing capabilities [1]. Their publication emphasizes the significance of real time monitoring and lightweight security systems, which is consistent with the necessity to perform dynamics anomaly detection within the medical support setting. Likewise, Rehman et al. offer the detailed overview of healthcare IoT innovations and security issues and state that the conventional security strategies cannot be applied to the dynamic medical systems [3]. Such researches formulate the incentive behind the incorporation of adaptive and real time detection policies.

Hybrid detection techniques have become a solution of interest as efficient solution to IoT security problems. Babar et al. present a hybrid deep learning based architecture as a way of enhancing the security and performance of healthcare IoT networks [2]. They indicate that the use of various methods of detection can make them stronger against different threats. This fact justifies the hybrid approach embraced in the proposed system regarding the combination of machine learning-based anomaly detection with rule based evaluation to enhance reliability.

A number of surveys are dedicated to the IoT security mechanisms and intrusion detection. The article by Szymoniak et al. is a review of defense techniques in the case of IoT systems and the importance of anomaly detection in the identification of unknown attacks [4].

Sebestyen et al. classify IoT security threats and underscore the need to monitor the behavior of devices and not just use signature based approach [5]. These reviews confirm the applicability of behavior based monitoring systems like the one applied in this project.

In the context of the Medical IoT, machine learning has been a popular topic when it comes to anomaly detection. Khan et al. present a safe IoMT architecture, which incorporates machine learning along with blockchain to guarantee the integrity of data and the safe processing [6]. Although blockchain poses an extra complication, the research paper has proven that machine learning is also effective in detecting abnormal behavior. The survey of federated learning methods to recognize anomalies in IoMT systems created by Pinto et al. emphasizes the importance of privacy protection and decentralized learning [7]. Despite the fact that federated learning has not been applied to the current project, their results confirm the appropriateness of unsupervised anomaly detection models in the medical setting.

Recent studies have also investigated edge level anomaly detection. Hizem et al. introduce an ECG anomaly detector to be deployed in edge devices used in Medical Internet of Things [8]. They focus their work on real time processing and low latency detection that is a key imperative in medical monitoring systems. Goumidi and Pierre introduce a real time anomaly detection model based on the ensemble learning models trained on healthcare specific datasets [9]. Their findings indicate that multiple learning models are more effective in detecting signals and this also endorses the usefulness of hybrid models.

Ensemble and hybrid intrusion detection techniques have also been studied in recent times. Chandekar et al. show the improved anomaly detection with the help of ensemble AI models in IoMT networks [10]. Abshari and Sridhar outline techniques of anomaly detection in cyber physical systems and note the efficiency of statistical, rule based, and learning based techniques in combination [11]. These works highlight the need to bring together various perspectives of detection to deal with compound attack situations.

Rule based systems remain very important in the IoT security since they are interpretable. In the article by Mehmmod et al., it is suggested that a machine learning-driven rule-based intrusion detection model can be applied in IoT settings, and it can be argued that rule based logic improves transparency and trust [12]. This argues in favor of the rule based risk assessment to be included in the suggested system, in which the alerts are properly explained to the user.

Hybrid cybersecurity solutions have been used in other areas besides the healthcare as well. Wang et al. present

a physical behavior analysis-based intrusion detection scheme of in vehicle systems [13]. Almalawi et al. examine hybrid approaches to cybersecurity measures towards industrial control systems [14]. The proposed hybrid intrusion detection method by Srivastav et al. applies to Industry 4.0 settings [15]. Despite the fact that these studies focus on various areas, they support the overall usefulness of hybrid detection structures.

To conclude, literature indicates that there is an increasing need of real time, interpretable, and hybrid security solutions to use in Medical IoT environments. Although most studies are based on complicated architectures or extensive datasets, lightweight and practical monitoring systems are still required. This gap is filled in the proposed project by incorporating data simulation, unsupervised anomaly detection, and rule based assessment into a real time dashboard to give a viable base of the Medical IoT cybersecurity research.

III.PROPOSED METHODOLOGY

Block Name	Description
Medical IoT Data Simulation	This block generates continuous device data such as heart rate, temperature, blood pressure, battery level, device ID, and timestamp. It supports both normal operation and attack scenarios to simulate real time Medical IoT behavior.
Real-Time Data Stream Handler	This block manages the incoming data stream and forwards each data instance to the detection modules without delay. It ensures smooth data flow for continuous monitoring.
Machine Learning Anomaly Detection	This block applies an unsupervised anomaly detection model to identify unusual patterns in heart rate and battery values. It produces an anomaly flag for each data record.
Rule-Based Risk Assessment	This block evaluates predefined security and operational rules such as abnormal vital ranges, low battery, identity mismatch, and timing errors to detect potential risks.
Alert Generation and Decision Logic	This block combines outputs from machine learning detection and rule- based assessment to generate clear and interpretable alert messages.
Real-Time Monitoring Dashboard	This block displays charts, alerts, device logs, system statistics, and mitigation options such as block and quarantine through an interactive user interface.

Table 1. Description of System Block Diagram Components

The given methodology outlines the systematic plan of the design and implementation of a real time system of monitoring cyber attacks on a simulated Medical Internet of Things device. The algorithm unites the data simulation, anomaly identification, and risk evaluation into a single monitoring process. All the components function in a ordered sequence and contribute to the overall process of detection and alert generation process.

A. IoT Data Simulation Medical.

The initial phase of the methodology is aimed at creating a continuous stream of Medical IoT device data to be reflective of the actual operating conditions of the world. Because the system is a prototype, real time production of synthetic data is done rather than stored datasets. The device readings that the simulation module produces include the heart rate, body temperature, blood pressure, battery level, and the timestamp information. These parameters have been chosen due to the fact that they are parameters normally tracked in medical wearables and can be utilized to track abnormal behavior.

The simulation is helpful in generating normal and attack driven data. Under normal operation, the values produced are within acceptable physiological and operation limits. In attack mode, the logic of data generation will suffer abnormal patterns depending on the chosen type of attack. Such patterns involve extreme vital values, unsteady readings or a low battery level in order to simulate malignant interference or equipment failure. A device identity and an attack indicator is also included in each record of data that can be used later in modules to determine integrity related conditions. Both the machine learning analysis and rule based evaluation take the continuous stream of data as input.

B. Anomaly Detection based on machine learning.

The second phase uses machine learning to detect anomalous behavioral patterns of the simulated devices data. An unsupervised anomaly detector model is applied to prevent the reliance on labeled training examples. The model

is then trained offline and loaded at the time of real time inference. The input features applied to detect an anomaly are selected device parameters, namely the heart rate and battery level since this aspect is sensitive to abnormal conditions.

The model compares the computed values to the normal behavior that has been learned to determine whether the observed values are abnormal in case of every incoming data instance. The result is a binary choice, which removes whether the current data point is anomaly or not. This detection layer also provides the system with the ability to detect unexpected patterns that might not have been formally addressed by a set of rules. The abnormality indicator produced by the model is attached to the data record and is sent to the subsequent analysis phase. This will increase the ability to detect as it captures behaviors that are subtle or that were not hitherto observed.

C. Rule Based Risk Assessment and Visualization.

The last step unites the rule based risk measurement and real time visualization and alert management. The rule based engine analyzes every record of data with a collection of predefined conditions concerning the behavior of the device, integrity, and operational conditions. These conditions are also checks of abnormal vital ranges, extremely low levels of battery, and inconsistencies in device identity, asynchronous time errors, signal disruptions, and operating time breaches. The anomaly flag generated by the machine learning model is also taken into consideration when the rules are evaluated with an aim of enhancing the confidence of the alerts.

According to the results of the evaluation, descriptive alert messages are created to define the identified risks. The output is presented in the form of an interactive dashboard built in Streamlit. The dashboard gives real time charts of device parameters, system statistics including alert counts and uptime and the latest device logs. Simulation involves the use of mitigation options, which include blocking the device and quarantine. This built-in visualization layer will guarantee that security incidents are well communicated and will facilitate the prompt decision making within a Medical IoT monitoring setting.

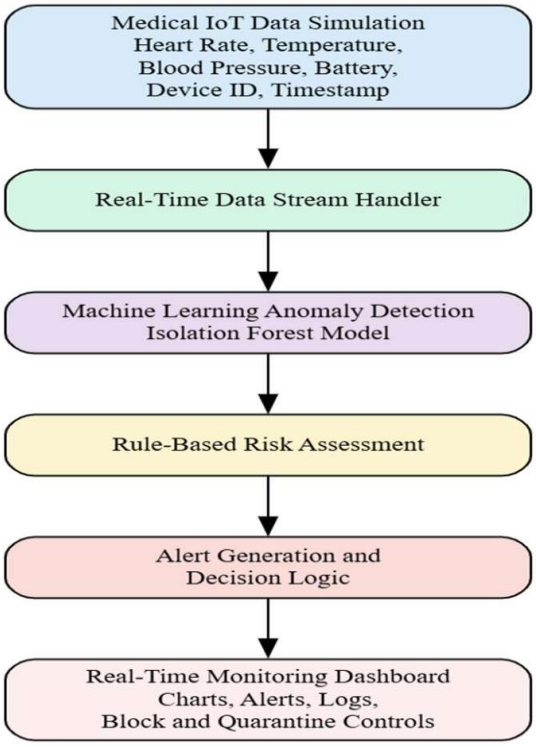

Figure 1: Block Diagram

IV.RESULTS AND DISCUSSIONS

In this section, the behavior of the proposed system of Medical IoT cybersecurity monitoring is observed in the conditions of simulation. The findings are addressed according to real time data generation, anomaly detection response, rule based alert generation and dashboard level observations. Because the system is a functional prototype, the system behavior and qualitative performance are discussed instead of those based on numerical measures of accuracy.

The simulated Medical IoT device generated steady physiological and operation data in normal operating conditions. The heart rate, temperature, blood pressure, and battery values were found to be within the anticipated parameters and system always reported the normal operational status. It is very unusual that the machine learning module identified anomalies in this phase and it means that the learned baseline behavior fits closely to the simulated normal data patterns. Minimal alerts were also generated by the rule based engine, which mainly was just a few checks on operations, like the hours of authorized working hours. This fact shows that the system does not cause too many false alerts when there is a stable functioning of the devices, and this is valuable to ensure that the operators do not lose trust.

Attack mode was enabled, and it was noticed that there were changes in the generated device data. The simulated values showed extreme values, decreased battery levels, or irregular values depending on the type of attack selected. The deviations were directly reflected on the dashboard charts where real time visualization of the abnormal behavior could be done. Heart rate and temperature line charts recorded sharp peaks and declines in case of data spoofing and floods whereas battery charts recorded faster reduced battery in case of signal related attacks. These visual patterns offered intuitive verification of deviant behavior of a device without the need to carefully examine raw logs.

These abnormal patterns were reacted well by the machine learning based anomaly detection module. Data points that were considered anomalous according to the model were registered when there was a significant change in the heart rate or battery values when compared to the behavior that it had previously learned. These anomaly flags were produced dynamically and added to the general alert process. The unsupervised character of the model also enabled it to discover irregularities even in cases where the characteristics that the exact nature of an attack were not clearly spelt out. This underscores the benefit of anomaly based detection in dynamic Medical IoT environments whereby attack behavior can be of different nature.

The rule based risk assessment engine had a complementary role of assessing a series of predefined security and integrity conditions. Rules about abnormal vital ranges, low level of batteries and known attack indicators were also often activated during attack simulations. The checks on the identity of the device and the validation of the timestamps allowed maintaining the consistency and authenticity of the data at all times. Besides, the randomness of simulated signal loss and heartbeat failures was added that represents real world uncertainty in wireless medical devices. These rule based alerts had clear explanations of issues that were found thus enhancing system interpretability.

Among the main findings of the findings, it can be noted the effectiveness of machine learning and rule based detection combination. The two detection layers in a number of situations provided data on the risks to be alerted on, which enhanced the confidence of the risks detected. Elsewhere, machine learning module identified minor abnormalities that were not explicitly outlined by rules. Rule based checks on the other hand captured operational violations which might not seem to be anomalous as per data distribution data. The hybrid method of detection minimized reliance on any particular method and enhanced the general penetration of possible security concerns.

The dashboard visualization also made the system much easier. Real time statistics like number of alerts, number of anomalies and the uptime of a system gave a brief overview of the device health. The latest device log table enabled an expedient review of the recent events, and the color highlighting enabled the attraction of attention to the important alerts. The alert messages were also presented with high priority to make sure that the abnormal conditions were not missed. The mitigation recommendations like device blocking or quarantine served to support proactive response planning although this was simulated.

The next critical issue that was realized in the course of system usage was the advantage of the session based state management. The system used persistent monitoring without using external databases or persistent storage. This made it much easier to deploy and it proved that with lightweight infrastructure it was possible to do effective monitoring. Nevertheless, long term analysis cannot be done due to the lack of storing historical data, which is understandable considering the prototype that is dedicated to real time monitoring of behavior.

It also shows that the simulation of synthetic data is a practical method of testing Medical IoT security mechanisms in controlled settings. The efficiency of detection logic may be tested by means of enabling various types of attacks and examining the reactions of the system without being exposed to actual patient data. The technique can also be useful in the initial system design and testing stages.

In general, the results obtained indicate that the suggested system can be used to combine real time data simulation, anomaly detection, rule based risk assessment, and visualization into one integrated monitoring solution. Although the system does not purport clinical or production level validation, it does provide a suitable demonstration of how hybrid detection strategies may help to facilitate cybersecurity awareness within the Medical IoT management setting. The discussion will bring out the practicality, interpretability and flexibility of the proposed approach, thus it is practical to use as basis of future research and development in the field of healthcare device security.

V.CONCLUSION

This was an actual time cybersecurity monitoring of a simulated Medical Internet of Things setting. The system has been created to meet the increasing demand of constant security awareness in healthcare equipment with limited resources and high availability demands. Combining the data simulation, anomaly detection, and rule based risk assessment in one dashboard, the project illustrates a viable method to track the behavior of medical devices and define the possible cyber risks.

The given system manages to demonstrate how synthetic Medical IoT data can be utilized to test security measures in the controlled environment. The simulation module produced continuous device readings which denoted normal and attack conditions. This enabled the system to monitor the alterations of behavior in key device parameters without the use of real patient data. This method can be especially useful when working at lower stages of development, where detection logic testing should be controlled.

The anomaly detection using machine learning helped the system to detect abnormal behavior patterns without having to use labeled datasets. The model unsupervised detection was found to be effective in showing the deviation of sensitive parameters like heart rate and battery level. This is useful in the context of Medical IoT where the new or

emerging threats need not be in a given pattern. Concurrently, the rule based risk assessment engine also provided the assurance that the operational and integrity checks, which were well understood, were applied on a regular basis. The combination of both techniques of detection guaranteed a wider coverage of the possible security concerns by the system.

Emphasis on interpretability and usability is another important result of this project. The dashboard implemented was the Streamlit based dashboard which was used to visualize in real time the behavior of the device, device alerts, and system statistics. The visual cues and clear alert messages allowed understanding the abnormal conditions in just a few seconds, which is necessary in a healthcare setting where the timely response is paramount. The simulated mitigation measures like locking out devices and quarantine was also included and it also provided the additional evidence of how monitoring systems are useful to aid the decision making in response.

Although the system is developed as a prototype and makes use of simulated data, it succeeds to demonstrate the possibility of real-life lightweight monitoring of cybersecurity of Medical IoT devices. The architecture can be devoid of intricate infrastructure dependencies and show it can be created with little to no resources in terms of resources. On the whole, this project underlines the systematic and feasible attitude towards Medical IoT security surveillance and can be used in the future to continue the investigation and improve cybersound healthcare device systems.

VI.FUTURE ENHANCEMENT

Although the suggested Medical IoT cybersecurity monitoring framework proves efficient in the area of real time identifying and visualizing functions, one can offer a number of improvements aimed at enhancing the functionality of the framework and its practical applicability. These enhancements include scalability, depth of detection and system flexibility without losing the light weight characteristic of the current design.

The feature set should be improved as one of the changes to implement to detect anomalies. The existing system takes into account a few parameters of the devices to perform machine learning. More functionality like the ability to track temperature changes, blood pressure fluctuations, etc, and temporal patterns in behavior would be useful in detection sensitivity. Multivariate analysis would enable the system to model more intricate interactions among device readings and be able to differentiate more between benign variations and malicious actions.

Adaptive learning mechanisms should be another possible improvement. The anomaly detecting model is now trained offline and is stationary as it is used. To make the system adapt to changing device use patterns, it may be useful to introduce periodic or incremental model updates depending on the behaviour of the normal ones. This would come in handy especially during long term deployments where the behavior of the devices might change with time depending on the environmental or operational conditions.

Refinement of the existing rules and the concept of contextual awareness can also be added to the rule based risk assessment module. The rules might be automatically modified according to the record of operations of the device, time of the day, or the number of alerts. This would minimize unnecessary alerts and enhance relevance of alerts. Also, it might be necessary to implement confidence level or severity scores of alerts to prioritize the responses in the case of high risk situations.

System architecture wise, the future versions may have secure storage of data in history to analyze it. The continuity of the chosen logs would facilitate trending, reviewing of incidents and post event investigation. Such an improvement would assist with a more thorough analysis of security events without violating the privacy of the data due to proper access control measures.

The dashboard interface may be also improved to multi device monitoring. At the moment, the system is concerned with one simulated device. It would be more realistic to extend the framework to support multiple devices which are required by real world Medical IoT. This would involve device level filtering, aggregated statistics and scalable visualization methods.

Lastly, work in the future can be done to introduce integration with real Medical IoT hardware or standard communication protocols. Although the given implementation is based on simulated data, the ability to get the system connected to real-life devices in controlled settings would confirm its applicability in practice. These improvements would bring the system nearer to actual deployment conditions but keep the main design principles of the system.

References

1. T. E. Ali, F. I. Ali, P. Dakić, and A. D. Zoltan, “Trends, prospects, challenges, and security in the healthcare internet of things,” Computing, vol. 107, no. 1, 2025.
2. M. Babar, M. U. Tariq, Z. Ullah, F. Arif, Z. Khan, and B. Qureshi, “An efficient and hybrid deep learning-driven model to enhance security and performance of healthcare internet of things,” IEEE Access, 2025.
3. A. U. Rehman et al., “Internet of Things in healthcare research: Trends, innovations, security considerations, challenges and future strategy,” International Journal of Intelligent Systems, 2025.
4. S. Szymoniak, J. Piątkowski, and M. Kurkowski, “Defense and security mechanisms in the Internet of Things: A review,” Applied Sciences, vol. 15, no. 2, 2025.
5. H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, “A literature review on security in the Internet of Things,” Computers, vol. 14, no. 2, 2025.
6. A. A. Khan et al., “BDLT-IoMT: A novel architecture for secure data processing in Internet of Medical Things,” Journal of Supercomputing, vol. 81, no. 1, 2025.

7. R. P. Pinto, B. M. Silva, and P. R. Inácio, "Federated learning for anomaly detection on Internet of Medical Things: A survey," Internet of Things, 2025.
8. M. Hizem et al., "Reliable ECG anomaly detection on edge devices for IoMT applications," Sensors, vol. 25, no. 8, 2025.
9. H. Goumidi and S. Pierre, "Real time anomaly detection in IoMT networks," IEEE Access, 2025.
10. P. Chandekar, M. Mehta, and S. Chandan, "Enhanced anomaly detection in IoMT networks using ensemble AI models," arXiv preprint, 2025.
11. D. Abshari and M. Sridhar, "A survey of anomaly detection in cyber physical systems," arXiv preprint, 2025.
12. A. Mehmmod et al., "ERBM: A machine learning-driven rule- based model for intrusion detection in IoT environments," Computers, Materials & Continua, 2025.
13. K. Wang et al., "ATHENA: An intrusion detection framework for in-vehicle systems," arXiv preprint, 2025.
14. A. Almalawi et al., "Hybrid cybersecurity for asymmetric threats," Symmetry, vol. 17, no. 4, 2025.
15. S. Srivastav et al., "HYRIDE: Hybrid and robust intrusion detection approach," Internet of Things, vol. 30, 2025.