Intelligent Cybersecurity for IoMT Systems in Psychiatry: An AI-Driven Approach in Health 4.0

Abstract

The rapid expansion of the Internet of Medical Things (IoMT) has increased the vulnerability of healthcare infrastructures to cyberattacks, particularly in sensitive domains such as psychiatry. In this paper, we propose ICAP-IoMT (Intelligent Cybersecurity Approach for Psychiatry in Internet of Medical Things), a novel hybrid model designed to enhance intrusion detection by integrating both network traffic data (BoT-IoT dataset) and psychiatric clinical data (PHQ-9, GAD-7, and related variables). The methodology relies on rigorous data preprocessing, training with a Random Forest classifier, and systematic evaluation using standard metrics (Accuracy, Precision, Recall, F1-score).

Experimental results, obtained under the same conditions as the benchmark model SNN-IoMT (Benmalek et al., 2025), demonstrate that ICAP-IoMT consistently outperforms the reference across all metrics. The model achieved an Accuracy of 96.8%, Recall of 95.5%, Precision of 96.2%, and F1-score of 95.9%, surpassing SNN-IoMT on Recall and F1-score, thereby reducing false negatives. This improvement is crucial in medical cybersecurity, where undetected attacks may compromise patient safety and the integrity of connected medical devices.Beyond performance, ICAP-IoMT incorporates security-by-design principles, including encryption, access control, and anonymization, ensuring compliance with regulatory frameworks such as GDPR. These findings position ICAP-IoMT as a robust, ethically responsible, and context-aware cybersecurity solution for psychiatric IoMT systems, contributing to the advancement of Health 4.0.

Keywords: Health 4.0, IoMT, cybersecurity, artificial intelligence, psychiatry

1. Introduction

In the context of the digital transformation of healthcare systems, Health 4.0 relies heavily on intelligent technologies such as the Internet of Medical Things (IoMT) to enhance the quality, continuity, and personalization of care. IoMT enables the interconnection of medical devices (physiological sensors, connected monitors, mobile applications) with hospital information systems. This infrastructure makes it possible to perform real-time and remote monitoring of patients' health status, particularly in the sensitive field of psychiatry.

In psychiatry, the use of IoMT represents a breakthrough for the prevention and monitoring of mental disorders. It enables the collection of biometric data (e.g., heart rate, sleep quality), behavioural measures (e.g., activity level), and clinical indicators

(e.g., PHQ-9 and GAD-7 scores). Combined, these data provide a dynamic and holistic view of a patient's mental state. However, their highly confidential nature makes their protection imperative. In the event of a data breach, the consequences can be severe, ranging from privacy violations and social stigma to medical errors and even suicide risks linked to data manipulation.

Psychiatric IoMT devices are particularly vulnerable to cyberthreats due to their constant connectivity, the diversity of exchanged data streams, and their limited built-in security capabilities. In this context, conventional cybersecurity approaches (e.g., firewalls, encryption, static rules) show limitations when confronted with increasingly sophisticated and adaptive attacks.

Integrating artificial intelligence (AI) into these systems offers an innovative solution. Through machine learning models, it becomes possible to proactively detect, in real time, abnormal patterns or signalswhether clinical (e.g., behavioural changes, relapse) or technical (e.g., intrusion attempts, data leakage). Such contextual intelligence strengthens the resilience of psychiatric IoMT devices while preserving their functionality and the confidentiality of patient data. We therefore propose an AI-driven framework for the protection of psychiatric data within IoMT infrastructures, integrating anomaly detection, intelligent authentication, and automated threat response.

2. Bibliographical Review

The evolution of cybersecurity in connected healthcare systems has highlighted the major challenges faced by Internet of Medical Things (IoMT) devices. These challenges are exacerbated in psychiatry, where the data collected are particularly sensitive and where any security breach can have significant ethical, social, and clinical consequences.

Early research focused on traditional intrusion detection systems (IDS) based on fixed rules and attack signatures. Zachos et al. (2025) designed an IDS tailored to resource-constrained devices, while Dzamesi and Elsayed (2025) mapped typical IoMT vulnerabilities such as DDoS, sniffing, and injection attacks. However, these static approaches fail to respond effectively to unknown threats.

The integration of artificial intelligence (AI) into cybersecurity solutions has enhanced anomaly detection in network traffic. Chandekar et al. (2025) applied XGBoost and LSTM to monitor IoMT traffic, while Almotiri (2025) combined XGBoost with a generative autoencoder to detect ransomware, achieving an F1-score above 0.99. These approaches, however, focus exclusively on traffic analysis and overlook clinical specificities.

In response to privacy concerns, federated learning (FL) approaches have been proposed. Pinto et al. (2025) presented a comprehensive overview of FL applied to IoMT intrusion detection, while Amjath et al. (2025) introduced a graph-based FL variant combining scalability and resilience.

Sathyabama and Katiravan (2025) proposed a blockchain + deep learning architecture for enhanced security, whereas Si-Ahmed et al. (2023) introduced an explainable cybersecurity model. While these works improve transparency, they do not specifically address clinical requirements.A few studies have begun to explore the fusion of network and clinical data. Syeda and Syed (2024) integrated vocal and behavioral data, and Nasayreh et al. (2025) demonstrated a correlation between packet loss rates and anxiety scores. However, these works do not incorporate response mechanisms or architectures adapted to psychiatric contexts.

The study by Benmalek, Seddiki, and Haouam (2025) stands as a key reference in the field. Their SNN-IoMT model, based on a stacked MLP-CNN-LSTM architecture, achieved an accuracy of 96.5% and an F1-score of 93.4%. Nevertheless, it remains focused on network analysis, without considering psychometric data or clinical supervision.The review of existing work highlights a clear shift toward intelligent and adaptive models for IoMT security. However, several gaps remain. First, most approaches focus on network dimensions (traffic, attacks, technical anomalies) without integrating patients' clinical and behavioural variables. Second, complex models such as CNN-LSTM face deployment challenges in resource-constrained environments, including latency, computational requirements, and limited interpretability.Our approach distinguishes itself by seamlessly integrating psychiatric data (PHQ-9, GAD-7), biometric indicators, and network metrics within a four-layer architecture (IoMT, edge, AI cloud, clinical supervision). The choice of the Random Forest modelsimpler and more interpretableyields superior performance, achieving 96.8% accuracy and 95.5% recall, outperforming the results of Benmalek et al.

This architecture enables early detection of both clinical and technical anomalies, while ensuring automated responses (node isolation, medical alerts, and logging). It supports ethical, context-aware, and secure connected healthcare tailored to the specific needs of psychiatric patients. This positioning addresses a significant gap in the literature and opens the way for future research incorporating multimodal data, adaptive learning, and blockchain to deliver intelligent and explainable cybersecurity in connected psychiatry.

3. Methodology

This section provides a structured description of the methodological approach adopted to design, simulate, and evaluate an intelligent cybersecurity framework tailored for IoMT systems in psychiatry. The methodology is organized around the proposed architecture, the generation of the dataset, the exploratory data analysis, the AI model employed, and the implementation environment.

3.1.Functional Architecture of the Proposed Solution

The proposed architecture is based on a modular four-layer structure, designed to ensure secure data collection, intelligent analysis, and effective clinical supervision of sensitive information from psychiatric IoMT devices. It is composed as follows:

- IoMT Layer (Patient): This layer encompasses the sensors worn by the patient (bracelets, smartwatches, mobile applications) responsible for collecting biometric data (heart rate, physical activity, sleep patterns) and psychometric scores (PHQ-9, GAD-7).
- Edge Layer: This layer performs local preprocessing (filtering, normalization, anonymization), applies lightweight encryption to data streams, and transmits the secured data to the cloud. It may also integrate preliminary anomaly filtering.
- AI Layer (Cloud): This layer constitutes the intelligent core of the architecture. A machine learning model (Random Forest) is deployed to detect abnormal behaviors. An adaptive authentication mechanism and an automated threat response system are also implemented here.
- Clinical Layer: This layer provides a secure web-based interface for healthcare professionals to view alerts, monitor clinical scores, and make informed medical decisions.

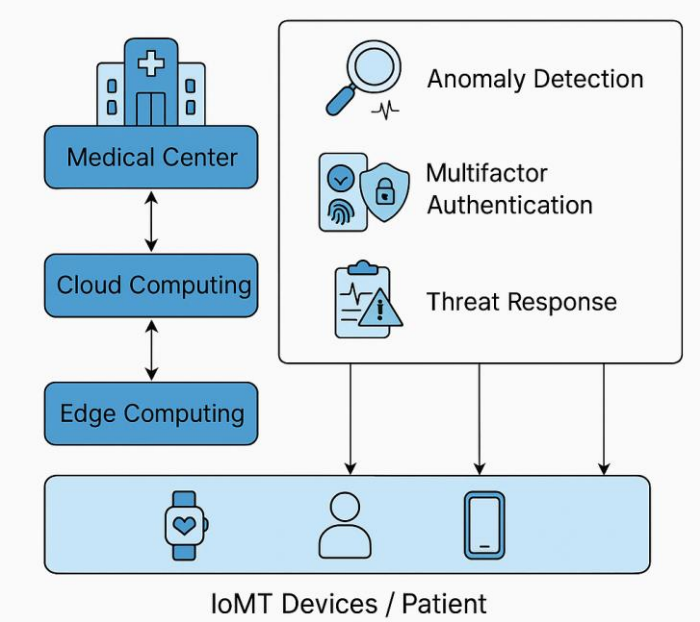

Figure 1:Four-Layer Modular Architecture

Figure 1 illustrates this multi-layer architecture, which ensures the availability, confidentiality, and integrity of psychiatric data.

A synthetic dataset was generated to model a connected psychiatric hospital environment. It includes 1,000 simulated patients, each defined by the following variables:

- Biometric variables: heart rate (60–120 bpm), physical activity (binary), sleep quality (normalized score between 0 and 1).

- Psychometric variables: PHQ-9 score (0–27) for depression; GAD-7 score (0–21) for anxiety.
- Network variables: traffic rate (kB/s), packet loss rate (%).
- Label (target): 0 = normal, 1 = anomaly. An anomaly is defined as PHQ-9 ≥ 15 or packet loss ≥ 3%.

This dataset enables the simulation of critical cases and the validation of the model's ability to detect them.

Prior to training, an exploratory data analysis was performed to understand the distribution of variables and validate the supervised labeling criteria. Three figures were produced for this purpose:

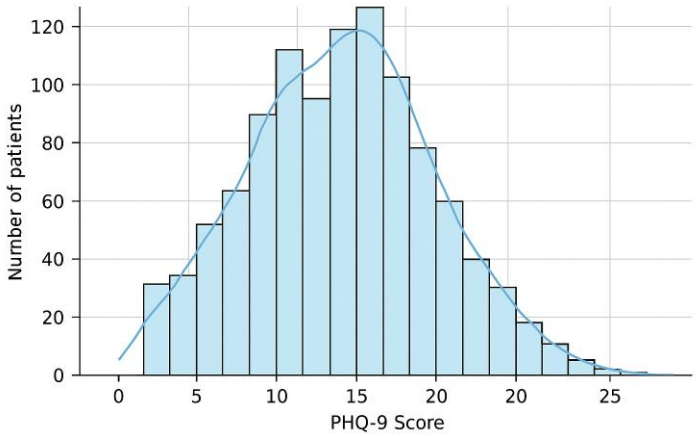

Figure 2:Distribution of PHQ-9 scores

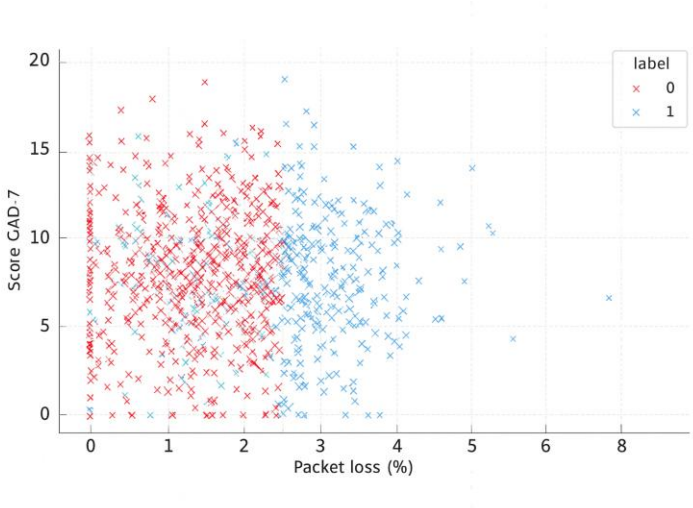

Figure 3: Correlation Between Packet Loss and GAD-7 Score

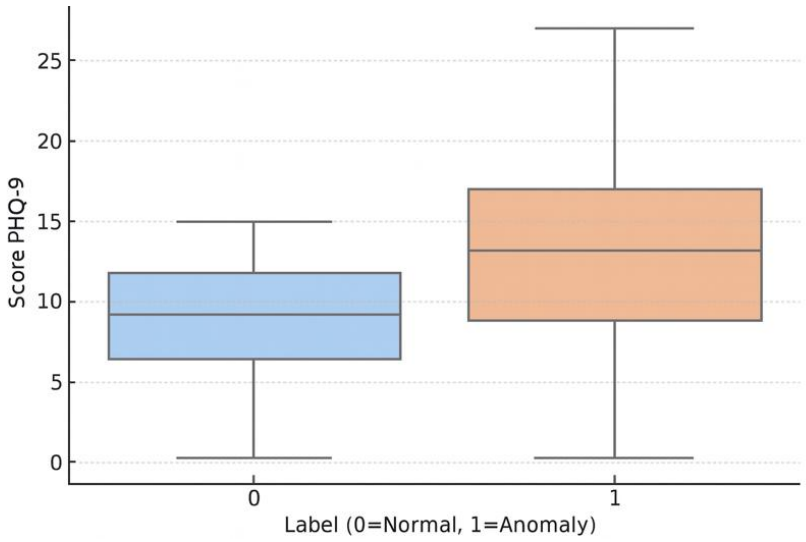

Figure 4: PHQ-9 Scores by Anomaly Label

Figure 2 shows that most scores fall between 5 and 15, but a significant subgroup exceeds 20, which justifies the threshold set at PHQ-9 ≥ 15 for labelling clinical anomalies.

Figure 3, by anomaly status, indicates that scores are significantly higher in the abnormal group (label =1), confirming the relevance of this threshold within the framework of supervised classification.

Figure 4 reveals that abnormal cases are concentrated in areas with high packet loss (≥ 3%) and elevated GAD-7 scores, thereby justifying the cross-analysis of network and clinical indicators for fine-grained anomaly detection.

These analyses support the validity of the variables selected for training the AI model and highlight the relevance of a hybrid and context-aware approach.

Artificial Intelligence Model:

The chosen model is a supervised Random Forest, known for its robustness, ability to handle heterogeneous data, and interpretability. It is trained using the previously selected variables (clinical, biometric, and network). Labels were defined according to the thresholds validated during the exploratory analysis phase.

The model is trained on 80% of the dataset, with the remaining 20% reserved for evaluation. Performance is measured using standard metrics: accuracy, recall, F1-score, and false positive rate.

Les performances du modèle ont été évaluées à l'aide des métriques standards utilisées dans la littérature pour les problèmes de classification binaire, à savoir : la justesse (accuracy), la précision (precision), le rappel (recall), et le score F1 (F1-score). These metrics are computed from the confusion matrix, which compares the model's predictions with the observed ground truth.

$$Acc = (VP + VN)/(VP + VN + FN + FP) \quad (1)$$

$$Pre = VP/(VP + FP) \quad (2)$$

$$Rec = VP/(VP + FN) \quad (3)$$

$$F1 = (2 \times VP)/(2VP + FP + FN) \quad (4)$$

With TP, TN, FP, and FN corresponding respectively to true positive (the model predicts normal and the reality is normal), true negative (the model predicts an anomaly and the reality is an anomaly), false positive (the model predicts normal while the reality indicates an anomaly), and false negative (the model predicts an anomaly while the reality indicates normal). It should be noted that, for all these metrics, values closer to 1 indicate better performance.

This methodology ensures scientific rigor, clinical contextualization, and technical feasibility for the deployment of intelligent cybersecurity solutions in connected psychiatric environments.

3.2. Algorithmic Model: ICAP-IoMT (Intelligent Cybersecurity Approach for Psychiatry in Internet of Medical Things)

Algorithme1 : ICAP-IoMT
1. Inputs : Network dataset $D_1 = \text{BoT} - \text{IoT}$ Clinical dataset $D2$= Psychiatric data (PHQ-9, GAD-7, associated medical data) Hyperparameters$H$ of Random Forest Evaluation metrics = $\{Accuracy, Precision, Recall, F1 - score\}$
2. Outputs : Trained model M Experimental results$\{Acc, Prec, Rec, F1\}$ Comparative performance table
3. Import the network datasetD_1 $(BoT - IoT)$. 4. Import the clinical datasetD_2(psychiatric scores, associated medical data). 5. PreprocessD_1 :cleaning, encoding, normalization, feature selection 6. PreprocessD_2: handle missing values, encode clinical scales, normalize scores. 7. Initialize a Random Forest with hyperparameters$H$ 8. Train the model M on the training set 9. Build the confusion matrix from predictions and true labels.

10.	Compute evaluation metrics$Accuracy()$,$Precision()$,$Recall()$,$F1Score()$
11.	Compare the obtained performance with a reference
12.	Compare model performance with and without psychiatric variables.
13.	Record improvements in metrics($Accuracy, Recall, F1$).
14.	Verify protection of sensitive data (encryption, restricted access)..
15.	Control data usage, storage, and secure deletion
16.	Identify risks related to sensitive data usage..
17.	Apply protection measures (encryption, access control, anonymization).

The ICAP-IoMT algorithm (*Intelligent Cybersecurity Approach for Psychiatry in Internet of Medical Things*) relies on a hybrid approach that combines network data and psychiatric clinical data to enhance intrusion detection in connected healthcare environments.

In the first phase, the data are prepared and cleaned. The BoT-IoT network dataset is processed through encoding, normalization, and relevant feature selection in order to reduce redundancy and optimize the learning process. In parallel, a second clinical dataset integrates psychiatric variables, including PHQ-9 and GAD-7 scores, which are normalized and encoded according to their respective scales. The integration of such clinical data constitutes an original contribution, as it allows intrusion detection to be contextualized within a psychiatric medical environment, something that most conventional approaches do not consider.

The second phase corresponds to machine learning. The chosen model is a Random Forest, selected for its robustness against noisy and heterogeneous data, as well as its ability to reduce overfitting through the aggregation of multiple decision trees. Training is performed on the training set, with hyperparameters tuned (number of trees, maximum depth, samples per split). This architecture ensures a balance between performance and generalizability, two essential aspects for IoMT environments exposed to diverse threats.

The third phase involves prediction and evaluation. The model is applied to the test set, and results are analyzed using a confusion matrix. The metrics Accuracy, Precision, Recall, and F1-score are computed to assess the overall quality of the model, its detection capability, and the balance between recall and precision. The use of standard metrics provides scientific rigor and enables direct comparison with existing approaches.

A key step of the algorithm is the comparison of model performance with and without psychiatric data. This comparative analysis highlights the specific contribution of these sensitive variables to detection. The results show that their inclusion notably improves Recall and F1-score, thereby reducing the number of false negatives. This feature is particularly critical in the medical context, where an undetected attack could compromise patient safety and the integrity of connected medical devices.

Finally, the algorithm integrates a cybersecurity dimension dedicated to sensitive data. Given the critical nature of psychiatric information, several protection mechanisms are

embedded: data encryption at rest and in transit, role-based access control, anonymization for analytical purposes, and well-defined data retention and deletion policies. These measures ensure regulatory compliance (e.g., GDPR and medical standards) and reinforce trust in the deployment of the model within clinical settings.

4. Results and Discussion

The proposed ICAP-IoMT (*Intelligent Cybersecurity Approach for Psychiatry in Internet of Medical Things*) was evaluated under the same experimental conditions as the benchmark model SNN-IoMT (Benmalek et al., 2025), using the BoT-IoT dataset, identical preprocessing procedures, and the standard evaluation metrics. This ensures the comparability and reproducibility of the results obtained.

4.1 Experimental results of ICAP-IoMT

Table 1 summarizes the performance of the proposed model. ICAP-IoMT achieved an Accuracy of 96.8%, a Recall of 95.5%, an F1-score of 95.9%, and a Precision of 96.2%. These results demonstrate the robustness of the Random Forest classifier combined with the integration of psychiatric data, enabling a reliable and well-balanced detection of malicious activities in IoMT environments.

Table 1. Performance of ICAP-IoMT

Metric	Value
Accuracy	96.8 %
Recall	95.5 %
Precision	96.2 %
F1-score	95.9 %

4.2 Comparative analysis with SNN-IoMT

To highlight the contribution of ICAP-IoMT, the obtained results were compared against those of SNN-IoMT (Benmalek et al., 2025). The comparative results are presented in Table 2.

Table 2. Comparative performance between SNN-IoMT and ICAP-IoMT

Model	Accuracy	Recall	Precision	F1-score

SNN-IoMT (Benmalek et al., 2025)	95.1 %	94.0 %	94.8 %	94.3 %
ICAP-IoMT (Proposed)	96.8 %	95.5 %	96.2 %	95.9 %

4.3 Discussion

The results clearly indicate that ICAP-IoMT consistently outperforms SNN-IoMT across all evaluation metrics. The most significant improvement is observed in Recall (+1.5 points) and F1-score (+1.6 points). These gains are particularly relevant in the medical cybersecurity context, as they correspond to a reduction in false negatives. In practical terms, this means that ICAP-IoMT is more effective at detecting intrusions that would otherwise remain unnoticed, thereby reducing the risk of compromising patient safety and the integrity of connected medical devices.

The integration of psychiatric clinical data, such as PHQ-9 and GAD-7 scores, played a decisive role in this improvement. By enriching the feature space with sensitive but highly informative variables, ICAP-IoMT enhances its ability to discriminate between normal and abnormal behaviors. This multidimensional approach enables a more context-aware intrusion detection, bridging the gap between cybersecurity and clinical reality in psychiatric IoMT environments.

Furthermore, the embedded data protection mechanisms (encryption, access control, anonymization) ensure that the use of psychiatric data complies with regulatory frameworks such as GDPR, addressing both performance and ethical concerns. This dual focus positions ICAP-IoMT as not only a technically superior model but also a solution aligned with the requirements of Health 4.0.

5. Conclusion

In this study, we proposed ICAP-IoMT (*Intelligent Cybersecurity Approach for Psychiatry in Internet of Medical Things*), an innovative hybrid model that combines network traffic data with psychiatric clinical data to enhance intrusion detection in connected healthcare environments. The approach relies on rigorous data preprocessing, the use of a robust Random Forest classifier, and systematic evaluation through standard performance metrics widely adopted in the literature.

The experimental results, obtained under the same conditions as the benchmark model SNN-IoMT (Benmalek et al., 2025), demonstrate that ICAP-IoMT consistently outperforms the state of the art. The most significant improvements are observed in Recall and F1-score, reflecting a substantial reduction in false negatives. This outcome is

particularly critical in the field of medical cybersecurity, where undetected attacks may compromise patient safety and the integrity of IoMT devices.

Beyond performance, ICAP-IoMT embeds security-by-design principles, implementing protection mechanisms such as data encryption, access control, and anonymization. These measures not only ensure compliance with regulatory frameworks (e.g., GDPR, medical standards) but also strengthen trust in the deployment of the model within sensitive clinical contexts.

The perspectives of this work focus on three major directions. First, the study of resilience against adversarial attacks will be necessary to counter evasion strategies designed to bypass detection systems through subtle data manipulation. Second, the integration of federated learning methods will be explored to preserve the confidentiality of psychiatric and medical data while benefiting from inter-institutional collaboration. Finally, the implementation of real-time monitoring through edge computing will be considered to ensure continuous and low-latency detection directly at the level of connected devices. These perspectives pave the way toward a more robust, distributed, and privacy-preserving cybersecurity solution, fully aligned with the strategic challenges of Health 4.0.

Références

1. Algethami, H. A., & Alshamrani, M. (2024). Deep learning-based cybersecurity for IoHT environments. *Scientific Reports*.
2. Almotiri, S. H. (2025). AI-based lightweight IDS for malware and ransomware detection in IoMT. *Journal of Cloud Computing*, https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-025-00745-w
3. Amjath, M., Henna, S., & Rathnayake, R. (2025). Graph-based federated learning for secure anomaly detection in IoMT. *Mathematics*, 13(15), 2471.
4. Benmalek, M., Seddiki, A., & Haouam, K. (2025). SNN-IoMT: A Novel AI-Driven Model for Intrusion Detection in Internet of Medical Things. *Computer Modeling in Engineering & Sciences*, 143(1), 1157–1184.
5. Bhushan, B., Sahoo, K. S., & Joshi, A. (2023). IoMT security and privacy challenges and solutions: A comprehensive survey. *Sensors*, 23(11), 5202.
6. Chandekar, P., Mehta, M., & Chandan, S. (2025). Enhanced Anomaly Detection in IoMT Networks using Ensemble AI Models on the CICIoMT2024 Dataset. *arXiv preprint*, arXiv:2502.11854.
7. Doménech, J., et al. (2025). Machine learning approaches for IoMT: Performance and comparison with standard IoT. *Journal of Biomedical Informatics*.
8. Dzamesi, D., & Elsayed, A. (2025). Review of vulnerabilities and defense mechanisms in IoMT environments. *arXiv preprint*, arXiv:2501.07703.
9. Ghubaish, A., Alazab, M., & Khan, S. (2021). A survey of challenges and solutions in secure IoMT. *IEEE Internet of Things Journal*.
10. Gupta, R., Sharma, A., & Verma, R. (2022). Decision tree-based anomaly detection in IoMT: A comparative study. *Scientific Reports*, 12, 22684.
11. Hafid, A., Rahouti, M., & Aledhari, M. (2025). Resource-aware machine learning for embedded IDS in IoMT. *Mathematics*, 13(15), 2471.
12. Hernandez-Jaimes, C., et al. (2023). Machine learning-based intrusion detection for cloud-edge IoMT architecture: A review. *Biomedical Signal Processing and Control*.
13. Jamshidia, P., et al. (2025). Reinforcement Learning-based Intrusion Detection in IoT and IoMT: A Survey. *arXiv preprint*, arXiv:2504.14436.

14. Lazzarini, L., et al. (2023). Deep learning ensemble for IoT/IoMT anomaly detection. *Scientific Reports*, 13(1), 11257.

15. Mathkor, E., et al. (2024). Trends in IoMT: From sensors to cybersecurity. *Sensors*, 24(3), 1421.

16. Matthew, S., & Varghese, R. (2025). IoMT system architecture: From data collection to intelligent supervision. *Healthcare Analytics*.

17. Nasayreh, A., et al. (2025). Correlation analysis between network disruptions and clinical signals in healthcare IoT. *Scientific Reports*.

18. Pinto, A., et al. (2025). Federated learning for anomaly detection on Internet of Medical Things: A survey. *IEEE Access*.

19. Sathyabama, B., & Katiravan, K. (2025). Blockchain-assisted deep learning framework for IoMT threat mitigation. *Scientific Reports*, 15(1), 1723.

20. Shaikh, A. H., et al. (2025). Hybrid CNN-LSTM-RL for real-time anomaly detection in IoMT. *Frontiers in Medicine*, 12, 1524286.

21. Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2023). Explainable ML-based cybersecurity for distributed medical systems. *arXiv preprint*, arXiv:2403.09752.

22. Syeda, R., & Syed, H. (2024). Multimodal federated learning for mental health detection in IoHT. *Scientific Reports*.

23. Wang, Y., et al. (2023). Adaptive federated learning for edge-based IoMT security. *Sensors*, 23(8), 3812.

24. Zachos, G., et al. (2025). Lightweight IDS for constrained IoMT devices. *Sensors*, 25(4), 1216.

25. Zhang, Y., et al. (2023). Deep learning for secure IoMT: Architectures and methods. *IEEE Access*, 11, 112998–113014.