A Binning-Based Approach for Intrusion Detection and Attack Classification in Internet of Medical Things Networks

Lerina Aversano, Stefano Galantucci(✉), Michele Mastroianni, and Andrea Porcelli

Department of Agricultural Sciences, Food, Natural Resources and Engineering (DAFNE), University of Foggia, Foggia 71122, Italy
{lerina.aversano,stefano.galantucci,michele.mastroianni, andrea.porcelli}@unifg.it

Abstract. Internet of Medical Things (IoMT) is redefining modern healthcare by enabling the continuous collection, transmission, and analysis of patient data through interconnected medical devices, wearables, and hospital systems. These advantages, however, extend and complicate the e-health attack surface, the effects of which are devastating as they impact human health and privacy. Reports indicate a rise in IoT-based cyberattacks targeting medical infrastructures and sensitive data regarding patients' health; consequently, Intrusion Detection and Prevention Systems (IDS/IPS) have become essential components of secure IoMT architectures. IoMT networks generally have different characteristics from traditional networks and require ad hoc solutions. Most IDS/IPS models in the literature rely on deep learning architectures that, while achieving high accuracy, are unsuitable for real-time operation in resource-constrained IoMT environments. The resulting gap between recognition performance and solution deployability leaves IoMT networks lacking real-world applicable approaches. To address this gap, this paper introduces a lightweight hybrid IDS/IPS framework that combines decision tree models with a compact neural network. The neural network is enhanced through a supervised binning mechanism designed to handle non-continuous and heterogeneous IoMT data effectively. Experiments on three widely adopted IoMT datasets (CICIoMT 2024, IoMT TrafficData, and WUSTL EHMS 2020) show that the proposed model achieves accuracy and F1-weighted scores exceeding 0.99, while processing 30,000–100,000 samples per second. Compared to state-of-the-art deep models, our approach maintains comparable or superior detection capability with significantly lower computational cost. The model proved to be particularly robust and effective in attack detection (binary classification) and attack classification (multiclass classification) tasks.

Keywords: Internet of Medical Things (IoMT) · Internet of Things (IoT) · Intrusion Detection and Prevention Systems (IDS/IPS) · E-health · Healthcare · Binning · Decision Tree · Neural Network

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2027
O. Gervasi et al. (Eds.): ICCSA 2026 Workshops, LNCS 16763, pp. 351–368, 2027.
https://doi.org/10.1007/978-3-032-30530-5_22

1 Introduction

The integration of interconnected devices into the healthcare domain, known as the Internet of Medical Things (IoMT) [4,26,54], is revolutionizing patient care by enabling continuous real-time monitoring and remote management of clinical data. These systems connect medical devices, wearables, gateways, and hospital information systems across wards, ambulances, and homes, so that data can flow where it is needed for timely decisions and safe treatment [10,39]. Modern IoMT architectures offer unprecedented advancements in personalized healthcare solutions, the continuous transmission of highly sensitive physiological data introduces severe privacy vulnerabilities. This rapid expansion, introduces critical cybersecurity vulnerabilities [13,15,44]. According to data obtained from SonicWall Capture Labs in 2022, over 112 million IoT cyber attacks have been reported worldwide [1]. The sensitive nature of health data and the direct impact on patient safety and personal information make IoMT systems a prime target [30,48] for attacks that can disrupt or degrade essential services. Attacks on IoMT systems can lead to catastrophic consequences. Breaches of confidentiality can result in the theft of health data, breaches of availability can cause the failure of devices that help to ensure patient health, and breaches of integrity can alter the functioning of devices, causing them to operate improperly. In the best-case scenario, this results in a serious privacy violation, while in the worst-case scenario, it can lead to the death of a device-using patient. In this context, the development of effective Intrusion Detection/Prevention systems (IDS/IPS) capable of identifying anomalies in real time is not merely a technical task but a requirement for keeping connected healthcare reliable and secure [22,47,59]. Over the years, a wide range of solutions for IDS/IPS systems has been developed [20,21,36,42,45,49,55,56], but these are aimed at generic or corporate networks. IoMT networks and, more generally, IoT networks exhibit different characteristics [14,17,58], different protocols [12,19], and different traffic flows and volumes. This implies that this research problem requires different approaches: from this perspective, research has explored many learning-based IoMT IDS/IPS solutions. Many works [11,16,18,19,29,38] propose deep learning models to capture complex, non-linear interactions in traffic and device behavior. For example, convolutional networks are used to learn temporal patterns [32,43], recurrent models [53] to capture longer dependencies, and newer architectures that even transform tabular data into image-like structures to be processed by vision models [3,7,53]. Other authors propose ensemble approaches [28,34,37] that combine different deep models to push accuracy as high as possible. However, these advances often come with trade-offs. Deep models achieve good performance but are slow to train and heavy to execute. Conversely, simple deep models on tabular data, although lightweight, often struggle to reach high scores [11,19]. The constraints of time and resources required are indeed fundamental: on the one hand, time can make a difference to the patient's life; on the other hand, IoMT solutions are not generally equipped with large computational resources, so they cannot easily handle heavy approaches. Authors in [6,28] emphasise the need for fast, lightweight solutions that guarantee real-time monitoring and

detection. IoMT supports "real-time monitoring" of patients [51]; consequently, IDS/IPS must also operate in real-time to be effective. In short, IoMT intrusion detection should balance effectiveness with practicality. This alignment between algorithm and context is key to building secure, trustworthy, and sustainable IoMT systems. To address these needs, this work proposes a lightweight but highly effective IDS/IPS solution for IoMT networks. The proposed approach consists of a combination of decision trees and a simple neural network. These families were chosen because trees have proven to be highly effective on IoMT data [11,19], particularly on tabular telemetry data [28,40], and are easy to inspect, while small neural networks can model non-linear patterns with modest computing requirements [38]. The goal is not only to maximize accuracy on a benchmark, but to deliver dependable detection that fits IoMT workflows and meets resource limits. The proposed approach has been tested on three datasets widely used in the IoMT literature [9,11,19], obtaining results that, in most cases, outperform those reported in the current literature. Furthermore, since the literature mainly proposes heavyweight approaches, our model guarantees real applicability even on small medical devices, providing a real increase in the level of security in the e-health field.

The key contributions of this work are:

- the proposal of an IDS/IPS methodology for detecting and classifying attacks in IoMT networks, based on trees and neural networks;
- the testing of this methodology on three widely-used IoMT datasets: CICIoMT2024 [19], IOMT-TrafficData [11], and WUSTL-EHMS 2020 [9];
- comparison of the results obtained with the current literature, with respect to standard metrics and model weighting.

This work is organized as follows: the proposed approach is described in Sect. 3, the related work are presented in Sect. 2, the experiments and related results are discussed in Sect. 4, and the conclusions are in Sect. 5.

2 Related Work

The growing diffusion of IoMT requires robust and efficient IDS, capable of mitigating ever-increasing threats, safeguarding sensitive patient data, and ensuring system integrity from vulnerabilities or attacks [13,15,44]. Research directions focus on enhancing accuracy and generalization capabilities, often overlooking important metrics such as inference time and training cost. The balance between metrics and computational efficiency, which distinguishes between fast (low-latency) and slow (high-latency) security solutions, characterizes this research field. Indeed, the main solutions can be split into two groups: "heavy" solutions that aim for maximum performance and "lightweight" solutions that seek a compromise. The primary area for the proposed work concerns the development of robust and fast solutions, essential for real-time monitoring and for IoMT devices with limited resources [32,34].

The subsequent paragraphs discuss machine learning models that are "lightweight" and commonly use aggressive feature engineering. This category includes Recursive Feature Elimination (RFE), used by [40] with 0.979 in test accuracy, 0.965 precision, and 0.863 recall with a DT. It also includes mixed approaches like RFE/MLP [38], which aim to minimize feature dimensionality with RFE and, at the same time, optimize the MLP, achieving 0.962 in every metric, consequently reducing computational overhead during training and inference. These two works use the dataset [9].

Similarly, the work of [33] highlights the effectiveness of feature selection based on Information Gain (IG) on the CICIoMT2024 dataset. This achieves with a MultiD-CNN the highest score in 5-fold cross-validation compared to many models, with a mean accuracy of 0.981, a mean precision of 0.977, a mean recall of 0.982, and a mean F1-score of 0.979. IG simplifies the dataset and improves classifier performance, but the MultiD-CNN model used exhibits high latency compared to other approaches.

The use of custom feature selection techniques based on mutual information, such as LRGU-MIFS [5], further emphasizes the push towards streamlining data complexity, reaching 0.949 in accuracy on the WUSTL-EHMS 2020 dataset [9]. Authors in [12] studied the behavior of these particular trees (Hoeffding DT) and other models on a dataset synthetically generated using IoT-Flock [25]. Hosain et al. [32] used XGBoost and XAI on WUSTL-EHMS 2020 [6], reaching the high accuracy score of 0.992. The approach proposed by Gupta et al. [28], which incorporates data augmentation on a random forest, has demonstrated exceptionally low latency on WUSTL-EHMS 2020 [9] with 0.942 accuracy, proving highly suitable for rapid detection scenarios. The Nilsimsa fingerprinting approach [31] provides a simplified modeling method for network traffic by bypassing the extensive feature extraction and selection phases commonly required by ML methods and using a hashing function, thereby increasing efficiency and achieving 0.982 accuracy on the CICIoMT2024 dataset. The goal of developing systems that are efficient in terms of resources and computational complexity, often incorporating lightweight ML classifiers such as Logistic Regression (LR) and K-Nearest Neighbors (KNN) into ensemble methods, remains fundamental for their implementability [9,34].

Conversely, in the literature, there are numerous Deep Learning (DL) architectures that often represent slower and more resource-intensive solutions, designed for maximum accuracy and to handle complex dependencies. Deep Learning (DL) models, while demonstrating superior performance in multi-class classification tasks (e.g., distinguishing 19 attack subtypes on the CICIoMT2024 dataset), frequently involve high prediction times or significant training overhead [16,29]. Examples include Convolutional Neural Network (CNN) models optimized for temporal analysis [43], achieving on CICIoMT2024 [19] 0.990 accuracy, 0.980 precision, 0.990 recall, 0.980 F1-score in multi-class classification, and 0.990 over all metrics in binary, demonstrating high performance although the convolutional layers are heavy. Deep Neural Networks (DNN) [29], and methods employing optimization algorithms such as Particle Swarm Optimization (PSO)

used in PSO-DNN models [18] on WUSTL-EHMS 2020, achieving 0.96 accuracy with a DNN, are recognized as computationally expensive [38,40]. Additionally, ensemble models are used [27]. Although the well-known cost in terms of computation in the IoT/IoMT environment, where efficiency is a must, evaluating the ten learning methods utilizing the TON_IoT [8] attack dataset, obtaining Matthews correlation coefficient (MCC) scores of 0.9971. The stacking-ensemble model emerged as the top performer. Highly advanced sequence modeling techniques, such as the use of Vision Transformers (ViT) in threat detection [7] reaching 0.995 across all metrics on the CICIoMT2024 dataset can be interesting from a theoretic point of view but unfeasible in real-world scenarios, or hybrid Recurrent Neural Networks (RNNs) like the BiGRU-BiLSTM proposed by [53] (0.999 on IoMT-TrafficData), CNN-LSTM hybridization proposed by [23] on [52], or the LSTM-based L2D2 (0.98 across all metrics on the CICIoMT2024 [19] dataset) model aiming for an optimal balance between accuracy and computational demand [3], yield high performance but increase architectural complexity and training time [38,46]. Features complexity reduction approaches drop irrelevant and redundant features from the dataset, enhancing model performance. However, efforts are being made to mitigate the latency of these models post-training through techniques such as model quantization, demonstrating low inference times even for complex hybrid DL models [53]. A critical research direction is the integration of these sophisticated models into distributed and privacy-preserving security architectures. This implies moving beyond centralized analysis towards systems that incorporate concepts such as Federated Learning (FL) and Blockchain [15,53]. The work of [37] proposes a multi-view learning approach within an FL setup to address scalability challenges and non-IID (non-independent and identically distributed) data inherent in real-world healthcare environments with an impressive accuracy score of 0.994 on the CICIoMT2024 [19] dataset. Migrating IDS models to real-world IoMT requires robust validation [32,34] and strict avoidance of data leakage [16]. However, current literature faces a persistent dichotomy: lightweight ML struggles with complex attacks, while deep learning (DL) imposes prohibitive computational overheads for edge deployment. Moreover, both frequently mishandle the heterogeneous, non-continuous nature of IoMT tabular data. Although feature discretization (*binning*) [24,41] is occasionally used in network security to simplify features [57], traditional unsupervised methods arbitrarily split data, discarding critical predictive signals. To bridge this gap, this paper introduces a hybrid solution leveraging a *supervised*, tree-based binning mechanism. By explicitly optimizing neural network performance on segmented data, our approach achieves DL-level accuracy while maintaining the minimal resource footprint vital for real-time medical device security.

3 Proposed Approach

The proposed approach is based on the hypothesis that the lower effectiveness [11,19] of simple neural networks (such as Multi-Layer Perceptrons, MLPs)

compared to tree-based algorithms in IoMT attack classification contexts is attributable to the intrinsic nature of certain features and to neural networks' difficulty in modeling non-continuous or piecewise decision functions. Recent studies [31,32,40] show that, especially with tabular data where features have heterogeneous semantics, tree-based algorithms are often more effective. The main idea behind the proposed approach is that this is not due to an intrinsic weakness of the neural model, but rather its inadequacy in natively handling categorical or numerical features that exhibit a "segmented" behavior—like IoMT data—without proper data preparation. The following examples help understand this issue:

- **Network Ports:** A feature representing a packet's destination port is categorical, as there is no numerical or ordinal relationship between port 80 (HTTP) and port 81; they are simply distinct identifiers. A decision tree can easily create a splitting rule like `port == 80` to isolate a specific behavior. A neural network, on the other hand, would struggle immensely if it received this feature as a single numerical value. It would have to learn, through linear combinations and non-linear activation functions (like ReLU), a complex function that isolates specific points on a numerical axis—an intrinsically difficult and inefficient task. The standard solution, one-hot encoding [50], can become impractical if the number of ports analyzed is very high.
- **Packet Length:** Although this is a continuous numerical variable, in certain contexts (like the Internet of Medical Things, IoMT), its behavior is not linear. Legitimate devices might communicate using packets within a very specific size range (e.g., 32–64 bytes). An attack, however, might use very small (e.g., < 10 bytes) or very large (e.g., > 1500 bytes) packets. This creates "zones of interest" that do not follow a linear progression. A decision tree can easily capture these intervals with rules like `32 < length < 64`. A neural network, in contrast, would have to model a function that behaves one way within an interval and another way outside of it, another task that requires the complex approximation of a step function.

In both cases, decision trees would achieve very high performance because their nature is to partition the feature space using thresholds and equalities, whereas neural networks are optimized for learning complex, continuous transformations of data. A possible solution proposed in this work is based on binning [35,41], which is a feature engineering process that converts continuous variables (x_j) into discrete representations (x'_j), also called feature discretization [24,57]. Binning can help in this particular context by improving robustness to outliers, decreasing overfitting, and handling important characteristics of features. This study employs a supervised, tree-based approach to create bins that are maximally informative about the target variable y.

The proposed methodology (illustrated in Fig. 1) is composed of the following phases:

1. **Ranking and selection of Top Features**: a preliminary Decision Tree T_{prelim} is trained on the full training set $D_{train} = (X_{train}, y_{train})$ to rank all

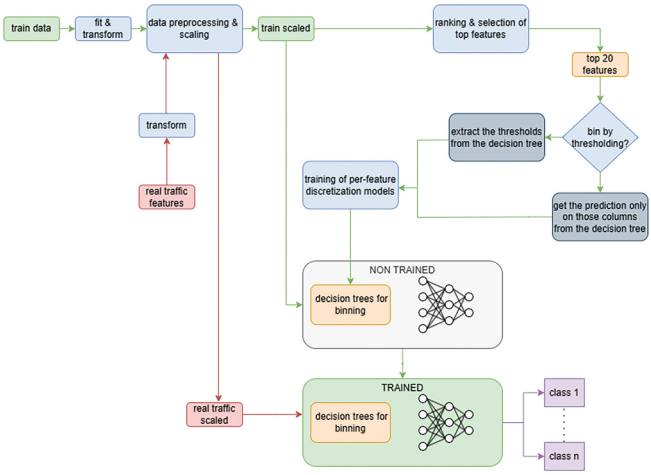

Fig. 1. Full operation of the proposed methodology.

features by their importance scores, I_j. Then, the top k features are selected to form the subset $X_{top\text{-}k}$;

2. **Training of Pre-Feature Discretization model**: for each feature $x_j \in X_{top\text{-}k}$, a dedicated, single-feature Decision Tree $T_j(\alpha)$ is trained. The model is trained using only the feature vector $\{x_j\}$ and the target vector y_{train};
3. **Feature Augmentation via Binning**: the trained trees $T_j(\alpha)$ are used to generate new binned features and augment the original datasets. This transformation is performed using two distinct techniques.
   - **Method A (Binning by Prediction)**: The new feature value is the tree's predicted class.

$$x'_{j,i} = T_j(\alpha).\text{predict}(x_{j,i})$$

   - **Method B (Binning by Thresholding)**: The new feature value is the index of the tree leaf where the sample lands.

$$x'_{j,i} = T_j(\alpha).\text{apply}(x_{j,i})$$

4. **Dataset preparation**: the binned feature set (e.g., $X_{\text{bin_pred, train}}$) are appended as new columns to the original feature matrix (e.g., X_{train}), thereby creating the final augmented feature matrix (e.g., $X'_{\text{pred, train}}$).
   - **For the Binning by Prediction method**:
     - Augmented **training set**: $X'_{\text{pred, train}} = [X_{train} \| X_{\text{bin_pred, train}}]$
     - Augmented **test set**: $X'_{\text{pred, test}} = [X_{test} \| X_{\text{bin_pred, test}}]$
   - **For the Binning by Thresholding method**:
     - Augmented **training set**: $X'_{\text{thresh, train}} = [X_{train} \| X_{\text{bin_thresh, train}}]$
     - Augmented **test set**: $X'_{\text{thresh, test}} = [X_{test} \| X_{\text{bin_thresh, test}}]$

where $\|$ denotes the horizontal concatenation of the feature matrices.

The binning in the third step can be interpreted from two perspectives:

1. **Threshold-Based Binning** [2]: From this viewpoint, each data point is allocated to a specific segment (or "bin") based on the path it takes through the tree's decision nodes. The internal nodes act as thresholds (for example: $X > 75$, $X > 100$, $X > 50$) that define the boundaries of these segments.
2. **Prediction-Based Binning:** This perspective focuses on the outcome. All data points that fall into the same segment are subsequently assigned the identical class label "like an ensemble" (e.g., 'malware' or 'goodware') defined by the terminal leaf node corresponding to that segment.

4 Experiments

This section details the comprehensive experimental design for this study. The hardware setup is provided in Sect. 4.1. The datasets employed are discussed in Sect. 4.2. The partitioning and validation strategy are provided in Sect. 4.3. The hyperparameter configurations are indicated in Sect. 4.4. The results of the experiments are reported and discussed in Sect. 4.5.

4.1 Hardware Setup

The experiments were conducted on a workstation equipped with an Intel Core i7-8700K processor, 32 GB of RAM, and an NVIDIA GeForce 5060 Ti GPU 16 GB VRAM. The deep learning models were implemented using TensorFlow v2.20-dev.

4.2 Datasets

To ensure a comprehensive and robust evaluation, three IoMT datasets were chosen, each offering a unique challenge in terms of data structure and attack representation:

- **CICIoMT2024** [19]: developed by the Canadian Institute for Cybersecurity (CIC), it consists of 18 different cyberattacks. A key strength of this dataset is its protocol heterogeneity, making it highly representative of current IoMT environments.
- **IoMT-TrafficData (2023)** [11]: It encompasses benign traffic generated by IoMT protocols like CoAP, MQTT alongside malicious traffic from 8 distinct attack types. Selected for its specific IDS focus, This study utilized its granular packet-based view.
- **WUSTL-EHMS 2020** [9]: From Washington University in St. Louis offers a unique perspective by combining network-level data with patient biometric data. Generated from a real-time Enhanced Healthcare Monitoring System (EHMS).The dataset focuses on Man-in-the-Middle (MitM) attacks, specifically spoofing and data injection.

Table 1. Class Distribution for the Considered Datasets

Dataset: CICIoMT2024 (19 Classes)				Dataset: IoMT-TrafficData (2023) (9 Classes)				Dataset: WUSTL-EHMS 2020 (2 Classes)			
#	Class/Attack Type	Samples	%	#	Class/Attack Type	Samples	%	#	Class/Attack Type	Samples	%
0	Spoofing ARP	17,791	0.20%	0	Normal	148,812	43.7%	0	Normal	14,278	87.50%
1	Benign	230,339	2.63%	1	Apache-Killer	24,000	7.0%	1	Attack (Spoofing + Alteration)	2,040	12.50%
2	MQTT DDoS connect flood	214,952	2.45%	2	RUDY	24,000	7.0%				
3	MQTT DDoS publish flood	36,039	0.41%	3	Slow-Read	24,000	7.0%				
4	MQTT DoS publish flood	52,881	0.60%	4	Slow-Loris	24,000	7.0%				
5	MQTT DoS connect flood	15,904	0.18%	5	ARP-Spoofing	24,000	7.0%				
6	MQTT Malformed data	6,877	0.08%	6	CAM-Overflow	24,000	7.0%				
7	Recon OS scan	20,666	0.24%	7	MQTT-Malaria	24,000	7.0%				
8	Recon Ping sweep	926	0.01%	8	Net-Scan	24,000	7.0%				
9	Recon Port scan	106,603	1.22%								
10	Recon VulScan	3,207	0.04%								
11	DDoS ICMP	1,887,175	21.51%								
12	DDoS SYN	974,359	11.10%								
13	DDoS TCP	987,063	11.25%								
14	DDoS UDP	1,998,026	22.77%								
15	DoS ICMP	514,724	5.87%								
16	DoS SYN	540,498	6.16%								
17	DoS TCP	462,480	5.27%								
18	DoS UDP	704,503	8.03%								

4.3 Data Partitioning and Validation Strategy

Evaluation protocols were aligned with dataset-specific conventions. CICIoMT2024 and IoMT-TrafficData were tested on both original and binary distributions to ensure comparability with prior studies [7,31]. Similarly, WUSTL-EHMS 2020 was converted to binary by merging attack classes, following established approaches [18,32,43]. Regarding validation, IoMT-TrafficData and WUSTL-EHMS 2020 employed Stratified 5-Fold Cross-Validation. Conversely, CICIoMT2024 utilized the original authors' fixed partitions [3,33,43] to prioritize direct benchmarking against existing literature over k-fold validation.

4.4 Hyperparameter Configuration

To ensure the reproducibility of all experiments, a global random seed was consistently applied across all model initializations and data partitioning. Our first evaluation compares four model families: a standard Decision Tree (DT), a baseline Neural Network (NN), and two NNs leveraging our augmented datasets (*Binned Prediction* and *Binned Thresholding*). The number of top features to be selected has been chosen as 20. This value ($\approx 50\%$ of the feature space of the datasets) is a pragmatic balance between model representativeness and computational cost. Literature [32,53] shows that this top quantile of features typically captures the majority of a dataset's predictive signal. Crucially, sensitivity analysis confirms this 20-feature threshold as the optimal trade-off: incorporating additional features yields negligible predictive gains while linearly inflating the memory footprint, resulting in an unjustified waste of storage and computational resources. All neural network models share a common textbook configuration 2. The number of epochs was selected in accordance with the observations in

[32,37,43], which show that this value is sufficient to achieve maximum performance; furthermore, this guarantees an overall reduction in time, which is a key factor in this study. The batch size was tailored to the dataset: 256 for the larger CICIoMT2024 and IoMT-TrafficData datasets, and 64 for the smaller WUSTL-EHMS 2020 dataset. Each hidden layer utilizes ReLU activation followed by Batch Normalization to stabilize training. The output layer employs Softmax or Sigmoid for multi-class and binary tasks, respectively. The Decision Tree was tuned over its `max_leaf_nodes` and `max_depth`, while the Binned NN variants include an additional hyperparameter, α, which controls the granularity of the binning process. The specific values explored for this comprehensive hyperparameter space are summarized in Table 2.

Table 2. Hyperparameter Space for All Models (Global Seed: `42`)

Family	Param	Values/Settings
DT	Max Leaves	{5, 10, 20, 50, 100, 200, 500, None}
	Max Depth	{5, 10, 15, None}
NN	*Fixed Params*	**Arch**: [128, 64, 32]; **BN**: Yes after each layer; **Epochs**: 20; **LR**: 1e-3
	Batch Size	**256** (CICIoMT, TrafficData), **64** (WUSTL 2020)
	Binned Models Specifics:	
	Binning α	{50, 100, 200, 500}
	Top-feat k	20

4.5 Results and Discussion

This section presents the performance evaluation of the models across the three datasets. The datasets were tested using the classes shown in Table 1.

As illustrated in the comparison graphs (Figs. 2, 3, and 4), which show the performance of the best configuration for each dataset and model, it can be affirmed that the hybrid approach improves overall performance. Our models demonstrated top-tier results across all three datasets, outperforming the Decision Tree and Neural Network that compose them. Specifically, BinThresh prevails in the CICIoMT2024 dataset, while BinPred is the highest performing model for the WUSTL-EHMS 2020 dataset. In the IoMT-TrafficData dataset, both BinPred and BinThresh rank first in a tie; however, their performance is comparable to that of the Decision Tree, surpassing it by only 0.001 in Balanced Accuracy.

Table 3 provides a comparison between the results obtained from this study and those from the current literature. Missing metrics are not stated in the listed studies: for this reason, no comparisons are proposed for these metrics; however, these are reported for greater transparency. To facilitate comparison with other studies, Table 3 also shows the values for an additional experiment, i.e., the testing of our models in binary attack/benign classification on CICIoMT2024 and IoMT-TrafficData. In this case, the values shown are those that correspond to

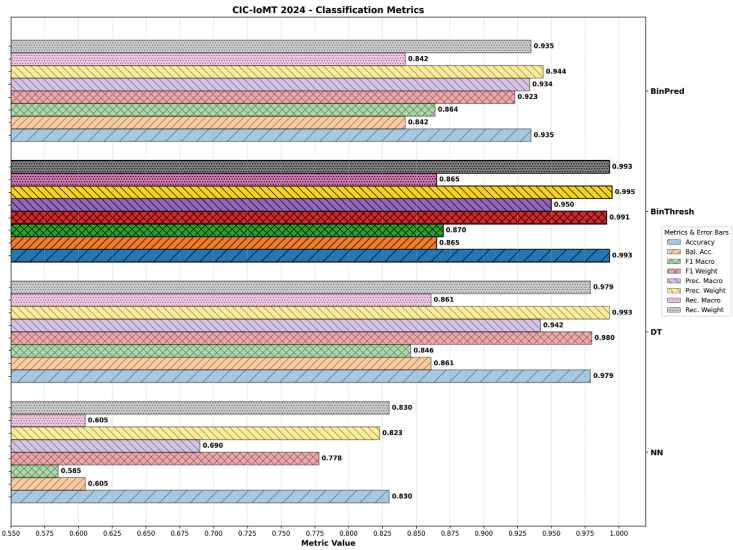

Fig. 2. Performance comparison between models (CICIoMT2024). For each metric, the value corresponding to the configuration that yields the highest result for that metric is reported. The variability in the bars refers to the variability observed between the folds in the same configuration.

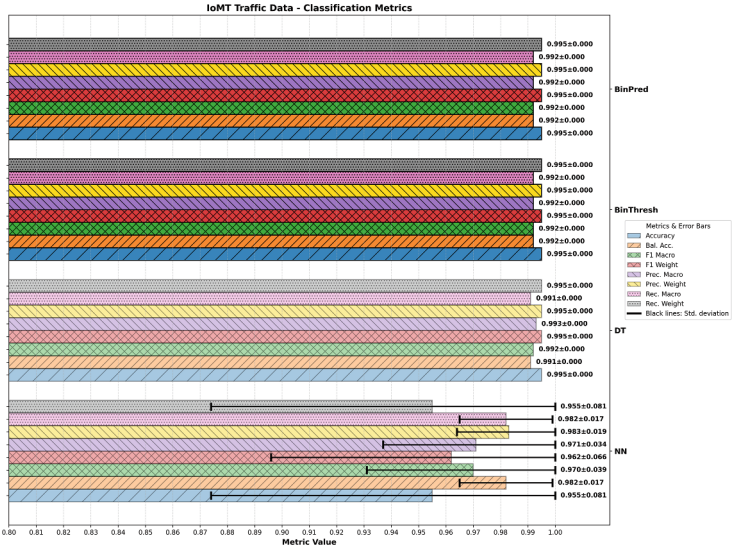

Fig. 3. Performance comparison between models (IoMT-TrafficData). For each metric, the value corresponding to the configuration that yields the highest result for that metric is reported. The variability in the bars refers to the variability observed between the folds in the same configuration.

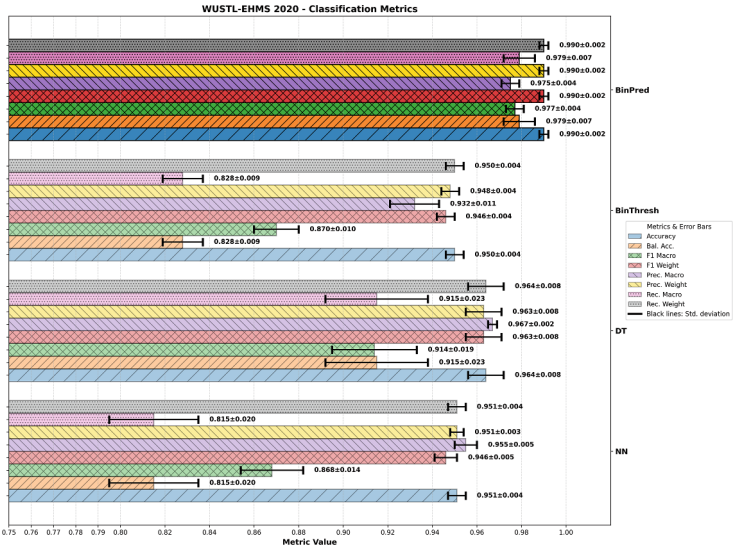

Fig. 4. Performance comparison between models (WUSTL-EHMS 2020). For each metric, the value corresponding to the configuration that yields the highest result for that metric is reported. The variability in the bars refers to the variability observed between the folds in the same configuration.

the model that achieves the best performance. For the CICIoMT2024 dataset, in the multi-class test, our approach achieves the best F1 Weight, Precision Weight, and Recall Weight metrics. Compared to the second-ranked CNN [43], it achieves an advantage of 0.011 in F1 Weight, 0.013 in Accuracy and Recall Weight, and 0.015 in Precision Weight. In accuracy, however, it is surpassed by [37] by 0.001. This is a perfectly acceptable margin considering that our approach is lighter in inference, thus allowing much more data to be processed in the IoMT scenario, where time is a critical factor. In the CICIoMT2024 test for binary classification, the best-performing model (BinThresh) achieves a remarkable 0.998 on F1 Weight, Precision Weight, Recall Weight, and Accuracy, surpassing the second-ranked model [7] by 0.003. It is meaningful that, both in the multi-class experiment and in the binary classification experiment, our approach outperforms computationally heavier models in inference [3,33,43]. Multi-class tests on the IoMT-TrafficData dataset show that the dominant model is the heavyweight XBiDeep [53], while our BinPred ranks second with a slight difference of 0.003 on Recall Weight and 0.004 on the other metrics. Given the minor difference in metrics, the lightweight nature of our model makes it an excellent solution in a real-world e-health context, offering an excellent trade-off between inference time and classification performance (0.995 across all compared metrics). It is also worth noting the great stability between folds. In the binary classification for IoMT-TrafficData, on the other hand, the proposed BinPred approach dominates all metrics, achieving an impressive 0.999 ± 0.000, outperforming other approaches

in terms of performance and lightweight nature. The tests for WUSTL-EHMS 2020 show more variable results. For F1 Weight, XAI-XGBoost [32] achieves the highest value with 0.991; however, our BinPred achieves a value of 0.990 ± 0.002, thus showing that there are folds where it outperforms XAI-XGBoost. Similar considerations apply to Precision Weight, where BinPred ranks first with a value of 0.990, tied with [16]; our variability leads it to exceed it by 0.002 in some folds. On Accuracy, our model achieves a score of 0.990 ± 0.002, which is slightly lower than the 0.992 achieved by XAI-XGBoost. XAI-XGBoost, on the other hand, dominates on Recall Weight with a score of 0.999. Even in this case, however, our model achieves excellent performance of at least 0.990 on all metrics in comparison, and is much lighter than [16,32], once again proving to be an excellent trade-off.

Table 3. Comprehensive Comparison of AI Models for Attack Detection in IoMT Environments

Study	Model	Inference Weight	Inf. Time (μs/samp)	F1 Weight	Prec. Weight	Rec. Weight	Acc.	F1 Macro	Bal. Acc.
Dataset: CICIoMT2024									
Multi-class Classification (19 Classes)									
L2D2 [3]	LSTM (2xLSTM + Dense)	Heavy	—	0.980	0.980	0.980	0.980	—	—
CNN-Based Detection [43]	CNN	Medium	—	0.980	0.980	0.990	0.990	—	—
InfoGain + MultiD-CNN [33]	MultiD-CNN (with IG)	Medium	—	0.979	0.977	0.982	0.981	—	—
Multi-view FL [37]	TabNet & MLP (Ensemble, FL)	Medium	—	—	—	—	**0.994**	—	—
CICIoMT2024 [19]	RF	Light-Medium	—	0.551	0.691	0.577	0.733	—	—
CICIoMT2024 [19]	LR	Light	—	0.432	0.547	0.471	0.727	—	—
CICIoMT2024 [19]	AdaBoost	Light	—	0.141	0.144	0.238	0.422	—	—
CICIoMT2024 [19]	DNN	Light	—	0.522	0.649	0.553	0.729	—	—
Our Study (BinThresh)	**Small NN + Bin Thresholding**	**Light**	9.0	**0.991**	**0.995**	**0.993**	0.993	0.870	0.865
Binary Classification (2 Classes)									
DDoSViT [2]	Vision Transformer (ViT)	Heavy	—	0.995	0.995	0.995	0.995	—	—
CNN-Based Detection [43]	CNN	Medium	—	0.990	0.990	0.990	0.990	—	—
Nilsimsa Fingerprinting [31]	RF (Nilsimsa)	Light-Medium	—	0.986	0.994	0.978	0.982	—	—
CICIoMT2024 [19]	RF	Light-Medium	—	0.961	0.971	0.951	0.996	—	—
CICIoMT2024 [19]	LR	Light	—	0.946	0.952	0.940	0.995	—	—
CICIoMT2024 [19]	AdaBoost	Light	—	0.959	0.959	0.961	0.996	—	—
CICIoMT2024 [19]	DeepNeuralNetwork	Light	—	0.952	0.956	0.948	0.996	—	—
Our Study (BinThresh)	**Small NN + Bin Thresholding**	**Light**	9.0	**0.998**	**0.998**	**0.998**	**0.998**	0.978	0.975
Dataset: IoMT-TrafficData									
Multi-class Classification (9 Classes)									
XBiDeep [53]	BI-GRU BI-LSTM	Heavy	—	**0.999**	**0.999**	**0.998**	**0.999**	—	—
IoMT-TrafficData [11]	RF	Light-Medium	—	0.994	0.994	0.994	0.994	—	—
IoMT-TrafficData [11]	DT	Light	—	0.951	0.970	0.938	0.938	—	—
IoMT-TrafficData [11]	LogR	Light	—	0.924	0.934	0.915	0.915	—	—
IoMT-TrafficData [11]	NB	Light	—	0.830	0.934	0.796	0.796	—	—
IoMT-TrafficData [11]	SVM	Light	—	0.918	0.922	0.915	0.915	—	—
IoMT-TrafficData [11]	DNN	Light	—	0.990	0.990	0.990	0.990	—	—
Our Study (BinPred)	**Small NN + Bin Prediction**	**Light**	7.9	$0.995_{\pm 0.000}$	$0.995_{\pm 0.000}$	$0.995_{\pm 0.000}$	$0.995_{\pm 0.000}$	$0.992_{\pm 0.000}$	$0.992_{\pm 0.000}$
Binary Classification (2 Classes)									
IoMT-TrafficData [11]	RF	Light-Medium	—	0.994	0.994	0.994	0.994	—	—
IoMT-TrafficData [11]	DT	Light	—	0.951	0.970	0.938	0.938	—	—
IoMT-TrafficData [11]	LogR	Light	—	0.924	0.934	0.915	0.915	—	—
IoMT-TrafficData [11]	NB	Light	—	0.830	0.934	0.796	0.796	—	—
IoMT-TrafficData [11]	SVM	Light	—	0.918	0.922	0.915	0.915	—	—
IoMT-TrafficData [11]	DNN	Light	—	0.990	0.990	0.990	0.990	—	—
Our Study (BinPred)	**Small NN + Bin Prediction**	**Light**	7.9	$\mathbf{0.999}_{\pm 0.000}$	$\mathbf{0.999}_{\pm 0.000}$	$\mathbf{0.999}_{\pm 0.000}$	$\mathbf{0.999}_{\pm 0.000}$	$0.999_{\pm 0.000}$	$0.999_{\pm 0.000}$
Dataset: WUSTL-EHMS 2020									
Binary Classification (2 Classes)									
PSO-DNN [18]	PSO-DNN	Heavy	—	0.950	0.960	0.960	0.960	—	—
Mutual Information FS [5]	LRGU-MIFS	Heavy	—	—	—	—	0.949	—	—
Towards Robust IoMT Models [16]	Deep Sequential Model	Heavy	—	0.990	**0.990**	0.990	0.990	—	—
XAI-XGBoost [32]	XGBoost (SMOTE-ENN)	Medium-Heavy	—	**0.991**	0.984	**0.999**	**0.992**	**0.990**	**0.990**
RFE-MLP [38]	RFE-MLP	Medium	—	0.962	0.962	0.962	0.962	—	—
A Tree Classifier Based IDS [28]	Robust Scaler + RF + Data augmentation	Light	3.5	0.938	0.935	0.909	0.942	—	—
RFE/Ridge [40]	RFE-DT	Light	—	0.911	0.965	0.863	0.979	—	—
IDS Comparison [29]	SVM	Light	—	—	—	—	0.924	—	—
Security Analysis [34]	Ensemble (LR + KNN)	Light	—	0.607	0.965	0.444	0.925	—	—
Our Study (BinPred)	**Small NN + Bin Prediction**	**Light**	28.6	$\mathbf{0.990}_{\pm 0.002}$	$\mathbf{0.990}_{\pm 0.002}$	$0.990_{\pm 0.002}$	$\mathbf{0.990}_{\pm 0.002}$	$0.977_{\pm 0.004}$	$0.979_{\pm 0.007}$

The inference time on the CICIoMT2024 and IoMT-TrafficData datasets is 9.0 and 7.9 μs/samp, respectively; this implies that they are capable of processing 111,000 and 126,582 examples per second, respectively. On the WUSTL-EHMS dataset, the times were longer (28.6 μs/samp). The remarkably low inference times measured for our model substantiate its suitability for real-time deployment in resource-constrained IoMT environments. It is important to contextualize this performance: while enterprise-grade IDS/IPS may prioritize terabit-scale throughput on network backbones, the defining challenge in

IoMT is achieving high-accuracy detection under strict computational limits. Our solution meets this challenge directly. With a throughput of over 34,000 classifications per second on the WUSTL-EHMS dataset and over 110,000 for the other two datasets, the system possesses orders of magnitude more capacity than required to process the predictable, low-volume flow data generated by a typical hospital ward of IoMT devices. Beyond inference efficiency, our model's minimal footprint ensures sustainable lifecycle costs and enables local retraining on hospital servers. While supervised binning mitigates overfitting by preventing noise memorization, detecting true zero-day anomalies remains challenging. Therefore, assessing robustness against unprecedented attacks requires future validation on continuous, real-world data streams. In conclusion, the proposed approach represents an optimal compromise between speed and classification performance.

5 Conclusions

This paper proposed a lightweight hybrid IDS/IPS approach that combines a decision tree model with a compact neural network architecture. The proposed methodology is driven by the insight that tree-based models excel at handling non-continuous and segmented feature spaces common in IoMT data, while neural networks can complement them by capturing subtle non-linear relationships. Through the introduction of a supervised binning process for feature discretisation, the approach improves robustness and computational efficiency without sacrificing detection accuracy. Experimental validation on three reference datasets (CICIoMT2024, IoMT-TrafficData, and WUSTL-EHMS 2020) confirmed the effectiveness of the proposed approach. In most cases, the hybrid methods (BinPred and BinThresh) outperformed or matched state-of-the-art, resource-intensive deep learning solutions while delivering inference times that fully support real-time operation. Specifically, our models achieved weighted F1 scores and accuracy scores above 0.99 in all the datasets, with the ability to process from 30,000 to 100,000 examples per second. These results demonstrate that lightweight models can achieve high-level performance while remaining usable for deployment on embedded or edge medical devices. In experiments where our methodology did not rank first in the metrics, it still achieved second place behind significantly heavier models. Tests conducted in both multiclass and binary classification showed the strength of the model in both recognising and classifying attacks in IoMT networks. While theoretically suitable for edge deployment, a current limitation is the lack of validation on physical IoT/IoMT hardware (e.g., ARM microcontrollers). Standard environments were used strictly to ensure benchmark comparability. Future work will prioritize on-device testing to evaluate real-world power consumption, thermal behavior, and exact hardware latency within a live hospital testbed. Furthermore, the variance calculated on the metrics showed the particular robustness of the model. In conclusion, our work shows how a solution that exploits the peculiarities of IoMT networks can be employed for the relative requirements of speed and accuracy in attack detection.

Acknowledgments. – **Funding:** This research was co-funded by the Italian Complementary National Plan PNC-I.1 "Research initiatives for innovative technologies and pathways in the health and welfare sector" D.D. 931 of 06/06/2022, "DARE - DigitAl lifelong pRevEntion" initiative, code PNC0000002, CUP: B53C22006450001.

– **Use of Generative AI:** The authors declare that no generative AI was used in the writing of the paper.

– **Data availability:** Data will be made available on request.

Disclosure of Interests. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Annual number of IoT attacks global 2022 | Statista — statista.com. https://www.statista.com/statistics/1377569/worldwide-annualinternet-of-things-attacks/. Accessed 11 June 06 2025
2. DecisionTreeDiscretiser — 1.9.3 — feature-engine.trainindata.com. https://feature-engine.trainindata.com/en/latest/user_guide/discretisation/DecisionTreeDiscretiser.html. Accessed 11 July 2025
3. Akar, G., Sahmoud, S., Onat, M., Cavusoglu, Ü., Malondo, E.: L2D2: a novel LSTM model for multi-class intrusion detection systems in the era of IOMT. IEEE Access (2025)
4. Al-Turjman, F., Nawaz, M.H., Ulusar, U.D.: Intelligence in the internet of medical things era: a systematic review of current and future trends. Comput. Commun. **150**, 644–660 (2020)
5. Alalhareth, M., Hong, S.C.: An improved mutual information feature selection technique for intrusion detection systems in the internet of medical things. Sensors **23**(10), 4971 (2023)
6. Alharthi, A., Alaryani, M., Kaddoura, S.: A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. Array, 100406 (2025)
7. Ali, M., Saleem, Y., Hina, S., Shah, G.A.: DDOSVIT: IoT DDOS attack detection for fortifying firmware over-the-air (OTA) updates using vision transformer. Internet Things **30**, 101527 (2025)
8. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A.: Ton_IoT telemetry dataset: a new generation dataset of IoTand IIoT for data-driven intrusion detection systems. IEEE Access **8**, 165130–165150 (2020)
9. Alsalman, D.: A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. IEEE Access **12**, 14719–14730 (2024)
10. Alsubaei, F., Abuhussein, A., Shandilya, V., Shiva, S.: IOMT-SAF: internet of medical things security assessment framework. Internet Things **8**, 100123 (2019)
11. Areia, J., Bispo, I.A., Santos, L., Costa, R.L.D.C.: IOMT-trafficdata: dataset and tools for benchmarking intrusion detection in internet of medical things. IEEE Access **12**, 115370–115385 (2024)
12. Aversano, L., Bernardi, M.L., Cimitile, M., Montano, D., Pecori, R., Veltri, L.: Explainable anomaly detection of synthetic medical IoT traffic using machine learning. SN Comput. Sci. **5**(5), 488 (2024)

13. Baho, S.A., Abawajy, J.: Analysis of consumer IoT device vulnerability quantification frameworks. Electronics **12**(5), 1176 (2023)
14. Benkhelifa, E., Welsh, T., Hamouda, W.: A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems. IEEE Commun. Surv. Tutorials **20**(4), 3496–3509 (2018)
15. Bhushan, B., Kumar, A., Agarwal, A.K., Kumar, A., Bhattacharya, P., Kumar, A.: Towards a secure and sustainable internet of medical things (IOMT): requirements, design challenges, security techniques, and future trends. Sustainability **15**(7), 6177 (2023)
16. Bouke, M.A., El Atigh, H., Abdullah, A.: Towards robust and efficient intrusion detection in IOMT: a deep learning approach addressing data leakage and enhancing model generalizability. In: Multimedia Tools and Applications, pp. 1–20 (2024)
17. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutorials **21**(3), 2671–2701 (2019)
18. Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., Bhushan, B.: A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things. Sustainability **14**(19), 12828 (2022)
19. Dadkhah, S., Neto, E.C.P., Ferreira, R., Molokwu, R.C., Sadeghi, S., Ghorbani, A.A.: CICIOMT 2024: a benchmark dataset for multi-protocol security assessment in IOMT. Internet Things **28**, 101351 (2024)
20. Dentamaro, V., Convertini, V.N., Galantucci, S., Giglio, P., Palmisano, T., Pirlo, G.: Ensemble consensus: an unsupervised algorithm for anomaly detection in network security data. ITASEC, pp. 309–318 (2021)
21. Elnakib, O., Shaaban, E., Mahmoud, M., Emara, K.: EIDM: deep learning model for IoT intrusion detection systems. J. Supercomput. **79**(12) (2023)
22. Eskandari, M., Janjua, Z.H., Vecchio, M., Antonelli, F.: PassBan ids: an intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet Things J. **7**(8), 6882–6897 (2020)
23. Faruqui, N., et al.: Safetymed: a novel IOMT intrusion detection system using CNN-LSTM hybridization. Electronics **12**(17), 3541 (2023)
24. Garcia, S., Luengo, J., Sáez, J.A., Lopez, V., Herrera, F.: A survey of discretization techniques: taxonomy and empirical analysis in supervised learning. IEEE Trans. Knowl. Data Eng. **25**(4), 734–750 (2012)
25. Ghazanfar, S., Hussain, F., Rehman, A.U., Fayyaz, U.U., Shahzad, F., Shah, G.A.: IoT-flock: an open-source framework for IoT traffic generation. In: 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), pp. 1–6. IEEE (2020)
26. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., Jain, R.: Recent advances in the internet-of-medical-things (IOMT) systems security. IEEE Internet Things J. **8**(11), 8707–8718 (2020)
27. Guo, G., Pan, X., Liu, H., Li, F., Pei, L., Hu, K.: An IoT intrusion detection system based on ton IoT network dataset. In: 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0333–0338. IEEE (2023)
28. Gupta, K., Sharma, D.K., Gupta, K.D., Kumar, A.: A tree classifier based network intrusion detection model for internet of medical things. Comput. Electr. Eng. **102**, 108158 (2022)
29. Hady, A.A., Ghubaish, A., Salman, T., Unal, D., Jain, R.: Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access **8**, 106576–106584 (2020)

30. Hathaliya, J.J., Tanwar, S.: An exhaustive survey on security and privacy issues in healthcare 4.0. Comput. Commun. **153**, 311–335 (2020)
31. Hernandez-Jaimes, M.L., Martínez-Cruz, A., Ramírez-Gutiérrez, K.A., Guevara-Martínez, E.: Enhancing machine learning approach based on nilsimsa fingerprinting for ransomware detection in IOMT. IEEE Access (2024)
32. Hosain, Y., Çakmak, M.: XAI-XGBOOST: an innovative explainable intrusion detection approach for securing internet of medical things systems. Sci. Rep. **15**(1), 22278 (2025)
33. Hossain, M.T., Meem, S.M., Setu, J.H., Halder, N., Islam, A., Alam, M.Z.: Cyber-attacks classification on internet of medical things using information gain feature selection and machine learning. In: 2024 Advances in Science and Engineering Technology International Conferences (ASET), pp. 1–10. IEEE (2024)
34. Ibrahim, M., Al-Wadi, A., Elhafiz, R.: Security analysis for smart healthcare systems. Sensors **24**(11), 3375 (2024)
35. Jacod, J.: Discretization of Processes, Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-24127-7
36. Jayalaxmi, P., Saha, R., Kumar, G., Alazab, M., Conti, M., Cheng, X.: Pignus: a deep learning model for ids in industrial internet-of-things. Comput. Secur. **132**, 103315 (2023)
37. Jeremiah, S.R., El Azzaoui, A., Gritzalis, S., Park, J.H.: Multi-view learning and model fusion framework for threat detection in multi-protocol IOMT networks. Inform. Fusion, 103435 (2025)
38. Kilincer, I.F., Ertam, F., Sengur, A., Tan, R.S., Acharya, U.R.: Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybernet. Biomed. Eng. **43**(1), 30–41 (2023)
39. Kotronis, C., et al.: Evaluating internet of medical things (IOMT)-based systems from a human-centric perspective. Internet Things **8**, 100125 (2019)
40. Lazrek, G., Chetioui, K., Balboul, Y., Mazer, S., et al.: An RFE/RIDGE-ML/DL based anomaly intrusion detection approach for securing IOMT system. Results Eng. **23**, 102659 (2024)
41. Liu, H., Hussain, F., Tan, C.L., Dash, M.: Discretization: an enabling technique. Data Min. Knowl. Disc. **6**(4), 393–423 (2002)
42. Mirlashari, M., Rizvi, S.A.M.: Enhancing IoT intrusion detection system with modified e-graphsage: a graph neural network approach. Int. J. Inf. Technol. **16**(4), 2705–2713 (2024)
43. Mohammadi, A., Ghahramani, H., Asghari, S.A., Aminian, M.: Securing healthcare with deep learning: a CNN-based model for medical IoT threat detection. In: 2024 19th Iranian Conference on Intelligent Systems (ICIS), pp. 168–173. IEEE (2024)
44. Mukhtar, B.I., Elsayed, M.S., Jurcut, A.D., Azer, M.A.: IoT vulnerabilities and attacks: silex malware case study. Symmetry **15**(11), 1978 (2023)
45. Musthafa, M.B., et al.: Optimizing IoT intrusion detection using balanced class distribution, feature selection, and ensemble machine learning techniques. Sensors **24**(13), 4293 (2024)
46. Naeem, H., Alsirhani, A., Alserhani, F., Ullah, F., Krejcar, O.: Augmenting internet of medical things security: deep ensemble integration and methodological fusion. Comput. Model. Eng. Sci. **141**(3), 2185 (2024)
47. Naghib, A., Gharehchopogh, F.S., Zamanifar, A.: A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities. Artif. Intell. Rev. **58**(4), 114 (2025)

48. Neto, E.C.P., Dadkhah, S., Sadeghi, S., Molyneaux, H., Ghorbani, A.A.: A review of machine learning (ml)-based IoT security in healthcare: a dataset perspective. Comput. Commun. **213**, 61–77 (2024)
49. Nie, F., Liu, W., Liu, G., Gao, B.: M2VT-IDS: a multi-task multi-view learning architecture for designing IoT intrusion detection system. Internet Things **25**, 101102 (2024)
50. Seger, C.: An investigation of categorical variable encoding techniques in machine learning: binary versus one-hot and feature hashing (2018)
51. Shammar, E., Cui, X., Zahary, A., Alsamhi, S.H., Al-qaness, M.A.: Threat to trust: a systematic review on internet of medical things security. J. Parallel Distrib. Comput. **206**, 105172 (2025). https://doi.org/10.1016/j.jpdc.2025.105172, https://www.sciencedirect.com/science/article/pii/S074373152500139X
52. Sharafaldin, I., Habibi Lashkari, A., Ghorbani, A.A.: A detailed analysis of the cicids2017 data set. In: Mori, P., Furnell, S., Camp, O. (eds.) International Conference on Information Systems Security and Privacy. ICISSP 2018. Communications in Computer and Information Science, vol. 977, pp. 172–188. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-25109-3_9
53. Turgut, Z., Başarslan, M.S.: XBIDEEP: a novel explainable artificial intelligence based intrusion detection system for internet of medical things environment. Internet Things, 101675 (2025)
54. Vishnu, S., Ramson, S.J., Jegan, R.: Internet of medical things (IOMT)-an overview. In: 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), pp. 101–104. IEEE (2020)
55. Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., Wang, J.: A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. PeerJ Comput. Sci. **9**, e1569 (2023)
56. Wang, Z., Li, J., Yang, S., Luo, X., Li, D., Mahmoodi, S.: A lightweight IoT intrusion detection model based on improved Bert-of-Theseus. Expert Syst. Appl. **238**, 122045 (2024)
57. Yoo, J., Min, B., Kim, S., Shin, D., Shin, D.: Study on network intrusion detection method using discrete pre-processing method and convolution neural network. IEEE Access **9**, 142348–142361 (2021). https://doi.org/10.1109/ACCESS.2021.3120839
58. Zarpelão, B.B., Miani, R.S., Kawakani, C.T., De Alvarenga, S.C.: A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
59. Zhong, M., Lin, M., Zhang, C., Xu, Z.: A survey on graph neural networks for intrusion detection systems: methods, trends and challenges. Comput. Secur. **141**, 103821 (2024)