information

MDPI

Article

HBiLD-IDS: An Efficient Hybrid BiLSTM-DNN Model for Real-Time Intrusion Detection in IoMT Networks

Hamed Benahmed [1,*], Mohammed M'hamedi [1,2], Mohammed Merzoug [1], Mourad Hadjila [3], Amina Bekkouche [1], Abdelhak Etchiali [1] and Saïd Mahmoudi [4,*]

1 LRIT Laboratory, Department of Computer Science, Faculty of Science, University of Abou Bekr Belkaïd, Tlemcen 13000, Algeria; mohamed.mhamedi@univ-tlemcen.dz (M.M.); mohammed.merzoug@univ-tlemcen.dz (M.M.); amina.bekkouche@univ-tlemcen.dz (A.B.); abdelhak.etchiali@univ-tlemcen.dz (A.E.)
2 Ecole Supérieure en Sciences Appliquées de Tlemcen, University of Abou Bekr Belkaïd, BP 165 RP Bel Horizon, Tlemcen 13000, Algeria
3 STIC Laboratory, Department of Telecommunication, Faculty of Technology, University of Abou Bekr Belkaïd, Tlemcen 13000, Algeria; mourad.hadjila@univ-tlemcen.dz
4 Computer Science Department, University of Mons, 7000 Mons, Belgium
* Correspondence: hamed.benahmed@univ-tlemcen.dz (H.B.); said.mahmoudi@umons.ac.be (S.M.)

Abstract

The Internet of Medical Things (IoMT) is revolutionizing healthcare by enabling continuous patient monitoring, early diagnosis, and personalized treatments. However, the het-erogeneity of IoMT devices and the lack of standardized protocols introduce serious security vulnerabilities. To address these challenges, we propose a hybrid BiLSTM-DNN intrusion detection system, named HBiLD-IDS, that combines Bidirectional Long Short-Term Memory (BiLSTM) networks with Deep Neural Networks (DNNs), leveraging both temporal dependencies in network traffic and hierarchical feature extraction. The model is trained and evaluated on the CICIoMT2024 dataset, which accurately reflects the diversity of devices and attack vectors encountered in connected healthcare environments. The dataset undergoes rigorous preprocessing, including data cleaning, feature selection through correlation analysis and recursive elimination, and feature normalization. Compared to existing IDS models, our approach significantly enhances detection accuracy and generalization capacity in the face of complex and evolving attack patterns. Experimental results show that the proposed IDS model achieves a classification accuracy of 98.81% across 19 attack types confirming its robustness and scalability. This approach represents a promising solution for strengthening the security posture of IoMT networks against emerging cyber threats.

Keywords: IoMT; IDS; preprocessing; deep learning; BiLSTM; multi-class classification

check for updates

Academic Editor: Georgios Kambourakis

Received: 15 June 2025
Revised: 20 July 2025
Accepted: 30 July 2025
Published: 6 August 2025

Citation: Benahmed, H.; M'hamedi, M.; Merzoug, M.; Hadjila, M.; Bekkouche, A.; Etchiali, A.; Mahmoudi, S. HBiLD-IDS: An Efficient Hybrid BiLSTM-DNN Model for Real-Time Intrusion Detection in IoMT Networks. *Information* **2025**, *16*, 669. https://doi.org/10.3390/info16080669

1. Introduction

The rapid expansion of the Internet of Things (IoT) industry and advancement in In-formation and Communication Technology (ICT) has significantly transformed the healthcare sector [1,2], through the widespread adoption of the Internet of Medical Things (IoMT), leading to improved remote patient care, enhanced diagnostic capabilities, real-time monitoring, and cost reductions [3]. However, the heterogeneous nature of IoMT ecosystems characterized by diverse operating protocols, lack of standardization in security implementations, and resource-constrained devices has created exploitable attack surfaces, making medical devices highly vulnerable and prime targets for cyber threats [4].

The critical nature of healthcare services and the privacy of medical data exacerbate security challenges in IoMT environments. Therefore, the need to provide protection against inappropriate access and attacks has become critical. Undetected anomalies in data traffic can have serious consequences, ranging from the tampering with diagnostic information [5], which can lead to serious medical problems such as delayed emergency care or even death [6], to physical damage from hardware failures, which can lead to partial or complete network downtime [7].

Intrusion detection systems (IDSs) are among the most widely available solutions for countering cyber threats in various IoT environments [8]. In healthcare environments, IDSs function as both an early warning mechanism and a primary defense layer by continuously analyzing network traffic to detect anomalies including hacking attempts, malware infections, and suspicious patterns and alerting healthcare providers of any potential security breaches at an early stage [9]. Due to the life-critical nature of healthcare services, the is growing demand for specialized IDS specifically designed to address the unique challenges of the IoMT.

In IoMT networks, medical devices and sensors generate data streams that exhibit both spatial and temporal dependencies [10]. Spatial patterns reflect device communication behavior [11], while temporal patterns capture the evolution of attack events over time [10]. Conventional IDSs are unable to address the unique characteristics of these environments. This includes their inability to effectively capture spatial and temporal patterns in network traffic and their inability to detect the dynamic and evolving nature of attacks in IoMT networks [12]. In particular, communication patterns between devices can fluctuate based on patient conditions, device configurations, and environmental factors, making it difficult for traditional IDSs to distinguish between benign and malicious activity, especially in real-time monitoring scenarios, where delays or inaccurate detection can have serious consequences for patient care [13]. This makes traditional IDS approaches unsuitable for IoMT security.

This study proposes HBiLD-IDS, a novel intrusion detection system (IDS) that addresses the critical challenge of securing Internet of Medical Things (IoMT) networks by analyzing complex spatio-temporal attack patterns with its pioneering BiLSTM-DNN hybrid architecture in diverse resource-constrained IoMT environments, offering distinct advantages over Conventional Neural Network (CNN) approaches which are limited to capturing spatial dependencies within data and Long Short-Term Memory (LSTM) approaches that process time sequences in a unidirectional manner only [14]. This hybrid approach was preferred over Transformers-based approaches, due to their higher computational demands which are unsuited for edge devices and their less effective generalization on smaller, domain-specific datasets in the IoMT ecosystem, and over Gated Recurrent Units (GRUs)-based approaches [15], which struggle to identify multi-stage intrusion patterns due to their limited memory capacity and for BiLSTM's superior ability to understand long-term dependencies and complete bidirectional context. HBiLD-IDS offer end-to-end protection with its BiLSTM layers that uniquely process attack sequences bidirectionally (forward and backward) [16], enabling superior detection of complex threats such as intermittent false data injection. The extracted spatio-temporal features are then refined by passing them to a DNN processor that analyzes attack signatures hierarchically [17], achieving exceptional classification accuracy that enables realistic discrimination between legitimate operations and intrusions. This unique architecture enables the system to proactively defend against intrusions. The HBiLD-IDS framework was evaluated using the CICIoMT2024 dataset, incorporating rigorous feature selection, while accounting for feature importance across different attack types to assess discriminatory power.

This paper is organized as follows: Section 2 reviews related works and identifies re-search gaps. Section 3 presents the methodology to develop the proposed model. First, it outlines the global framework and then introduces the CICIoMT2024 dataset and details the data preprocessing steps. Finally, it describes the detailed architecture and experimental setup. Section 4 presents and analyzes the obtained results and discusses limitations and suggests future enhancements. Section 5 concludes this study by summarizing key findings and contributions.

2. Related Work

Over the past few years, various machine learning (ML) and deep learning (DL) techniques have been proposed to enhance attack detection in IoT and healthcare-based systems using different benchmark datasets.

Shaikh et al. [18] proposed combining CNN, LSTM, and reinforcement learning models into a hybrid framework applied to the CICIoMT2024 dataset, achieving 77.73% accuracy for 19-class classification. In contrast, Sharma and Shambharkar [19] significantly improved performance to 98.56% using CNN, Recurrent Neural Network (RNN), and attention mechanisms on the same dataset, demonstrating the advantage of attention-based architectures. Similarly, Akar et al. [20] combined DNN and LSTM to reach 98% accuracy on the same multi-class dataset, confirming the effectiveness of hybrid sequential models.

Transformer-based models have gained significant attention due to their superior modeling of sequential and contextual features. Naeem et al. [21] implemented Transformer-based neural networks alongside DCNNs, LSTM, and meta-learners, achieving 98.84% accuracy for binary classification across WUSTL-EHMS-2020 and CICIoMT2024 datasets. Tseng et al. [22] and Alsharaiah et al. [23] also employed Transformer-based models, attaining accuracies of 99.40% and 99.71%, respectively, across CICIoT2023 and CICIoMT2024 datasets, always in binary classification, with the latter incorporating SHAP-based explainability to improve model transparency.

LSTM remains a foundational model for temporal sequence analysis in network traffic data. Faruqui et al. [24] applied CNN and LSTM across CICIDS2017/2018/2019 datasets, achieving 97.63% accuracy in a 12-class classification setup. Gueriani et al. [25] used CNN-LSTM on CICIoT2023 datasets, attaining 98.42% for binary classification. Other standalone LSTM-based approaches, such as the one proposed by Sayegh et al. [26], reached 99.75% accuracy on datasets including NSL-KDD and UNSW-NB15 for binary classification, while Jony et al. [27] reported 98.75% for 35-class classification using LSTM on CICIoT2023.

Ensemble-based methods such as Random Forest, XGBoost, and Decision Trees have also shown strong performance, particularly in multi-class contexts. Lipsa et al. [28] evaluated these models across CICIDS2017 and NSL-KDD datasets, achieving up to 99% and 99.80% accuracy for 14 classes and 05 classes, respectively. Talukder et al. [29] extended this evaluation to multiple datasets including UNSW-NB15, CICIDS2017, and CI-CIDS2018, achieving near-perfect accuracy across 10–15 classes using various ensemble models.

Furthermore, federated learning and explainable AI approaches have recently gained traction. Abbas et al. [30] introduced a federated DNN that achieved 99% binary classification accuracy on CICIoT2023, addressing privacy concerns by eliminating centralized data processing. Alsharaiah et al. [23] employed explainable AI using SHAP values with a Transformer-based DL model, combining interpretability with high accuracy on the CI-CIoMT2024 dataset.

Multi-dataset evaluation has emerged as a key approach to test generalization capability. Doménech et al. [31] achieved 99.85% accuracy on CICIoT2023 and CICIoMT2024 for a 6-class problem using classical ML models, while Khanday et al. [32] tackled 35-class classification with an LSTM and 1D-CNN approach, reporting 99.87% accuracy. These examples highlight the community's shift toward solving complex, real-world multi-class problems.

Finally, emerging architectures like GRU with attention mechanisms, as seen in the work of Saran et al. [33], have reached up to 99.99% accuracy on ICU datasets. Anwar et al. [34] incorporated federated learning with LSTM across WSN-DS, CICIDS2017, and UNSW-NB15, reporting 97.80% accuracy. These works indicate a growing interest in scalable, adaptive, and privacy-preserving solutions for intrusion detection in IoT and healthcare networks.

In summary (Refer to Table 1), the literature reveals a clear progression toward advanced, hybrid Deep Learning architectures with attention mechanisms and Transformer models, supported by privacy-conscious frameworks such as federated learning. While binary classifiers tend to reach high accuracy levels, multi-class classifiers are increasingly being prioritized for their practicality in real-world deployment scenarios.

Table 1. Summary of related work in IDS.

Authors	Year	Experimental Dataset	Techniques and Models	Classification Types	Accuracy
Shaikh et al. [18]	2025	CICIoMT2024	CNN, LSTM, and RL	Multi-class (19)	77.73%
Sharma and Shambharkar [19]	2025	CICIoMT2024	CNN, RNN, and Attention mechanism	Multi-class (19)	98.56%
Akar et al. [20]	2025	CICIoMT2024	LSTM	Multi-class (19)	98%
Naeem et al. [21]	2024	WUSTL-EHMS-2020, CICIoMT2024	Transformer-based DCNNs, LSTM, and Meta-learner	Binary	98.84%
Tseng et al. [22]	2024	CICIoT2023	Transformer Model	Binary	99.40%
Alsharaiah et al. [23]	2025	CICIoMT2024	Transformer-based DL and Explainable AI	Binary	99.71%.
Faruqui et al. [24]	2023	CICIDS2017, CICIDS2018 and CICIDS2019	CNN and LSTM	Multi-class (12)	97.63%
Gueriani et al. [25]	2024	CICIoT2023 and CICIDS2017	CNN and LSTM	Binary	98.42%
Sayegh et al. [26]	2023	CICIDS2017, NSL-KDD and UNSW-NB15	LSTM	Binary	99.75%
Jony et al. [27]	2024	CICIoT2023	LSTM	Multi-class (35)	98.75%
Lipsa et al. [28]	2025	CICIDS2017 and NSL-KDD	Random Forest, XGBoost, Decision Tree, and Support Vector	Multi-class (14)	99%
Abbas et al. [30]	2023	CICIoT2023	Federated DNN	Binary	99.00%
Doménech et al. [31]	2025	CICIoT2023 and CICIoMT2024	ML models	Multi-class (6)	99.85%
Doménech et al. [32]	2025	CICIoT2023 and CICIoMT2024	ML models	Multi-class (6)	99.85%
Saran & al. [33]	2024	NF-TON-IoT and ICU	Gated Recurrent Unit (GRU) and Attention Mechanism	Binary	99.99%
Anwar et al. [34]	2025	WSN-DS, CICIDS2017 and UNSW-NB15	FL-based LSTM	Binary	97.80%
Our Proposed Model (HBiLD-IDS)	2025	CICIoMT2024	Hybrid BiLSTM-DNN	Multi-Class (19)	98.81%

3. Methodology

This section presents the methodological framework of our HBiLD-IDS (Hybrid Bidirectional LSTM—Intrusion Detection System) architecture (Figure 1), a novel security model specifically designed for IoMT environments.

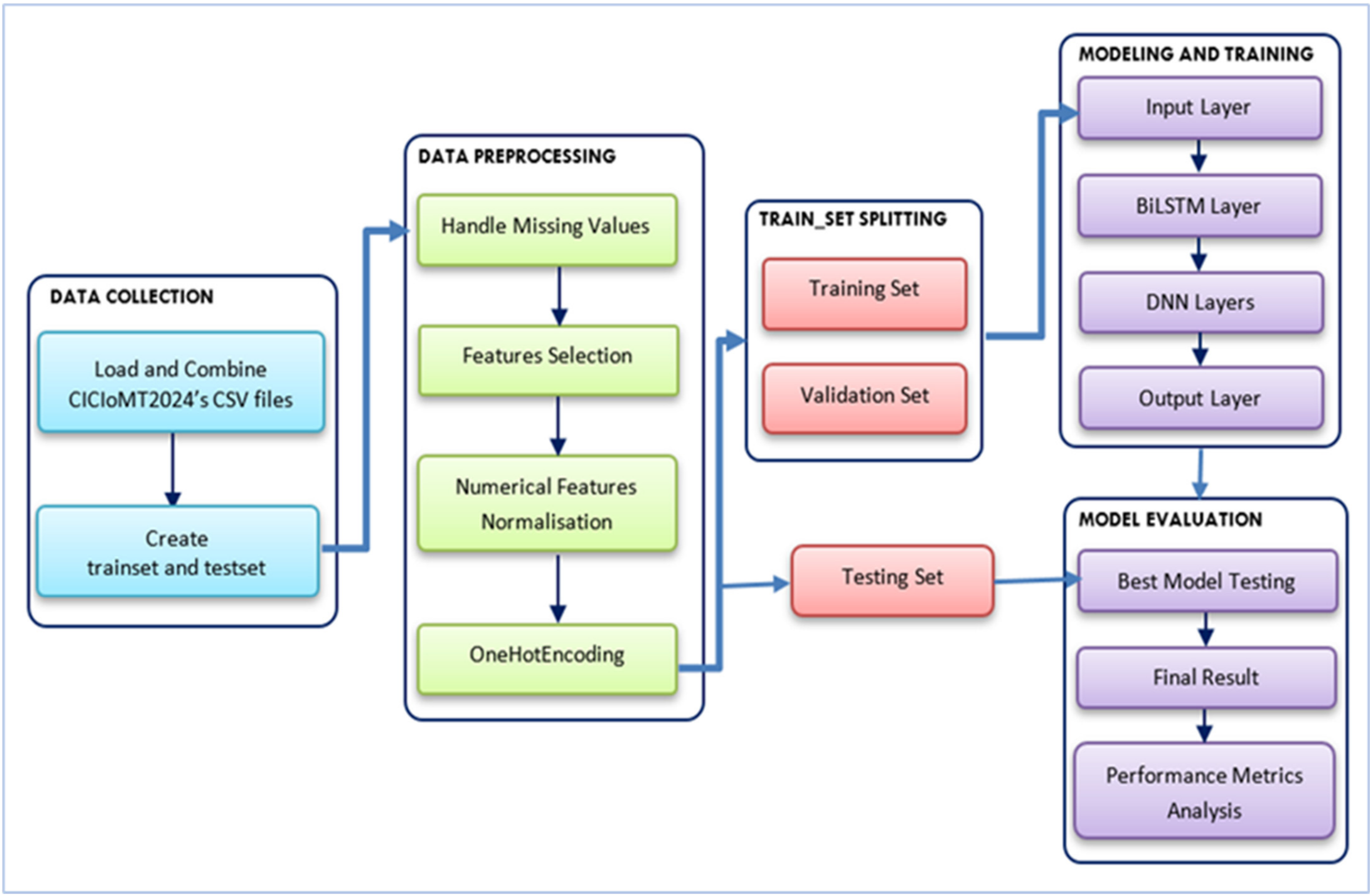

Figure 1. Proposed HBiLD-IDS model.

3.1. Dataset

In this study, we evaluate the proposed intrusion detection algorithms and models using the CICIoMT2024 dataset, a specialized benchmark for IoMT security research, curated and released by Dadkhah et al. [35] at the Canadian Institute for Cybersecurity (CIC); it combines (1) healthcare-specific attacks (e.g., medical device hijacking), (2) true multiprotocol traffic (WiFi, MQTT, and Bluetooth interactions), and (3) diverse clinical environments addressing critical gaps in existing datasets like CICIDS2017 (general network attacks only) and WUSTL-EHMS (limited to BLE protocols). This dataset provides realistic, annotated scenarios across mixed medical IoT ecosystems and enables precise detection model training for healthcare-specific threats.

3.1.1. Dataset Description

The CICIoMT2024 dataset includes network traffic captured from 40 IoMT devices, including 25 real devices (WiFi and Bluetooth protocol) and 15 simulated devices (MQTT protocol), representing the majority of devices commonly used in healthcare environments. Eighteen (18) different attack scenarios were observed, categorized into five main types: DDOS (distributed denial of service), DOS (denial of service), Recon (Reconnaissance), MQTT-based attacks, and Spoofing. Benign traffic is also captured in a zero-attack day for more balancing between malicious and non-malicious activities (given in Table 2). This allows for three classifications: binary (02 classes: benign and malicious), category level (06 classes: benign and 5 categories), and detailed (19 classes: benign and 18 subcategories), all aligned with the STRIDE threat model, a widely adopted cyber security framework categorizing threats into six core types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [36]. The collected data contains 8,775,013 instances characterized by 45 attack-aware features (as described in Table 2).

Table 2. Raw data distribution in CICIoMT2024 dataset according STRIDE model.

Binary	6-Classes	19-Classes	Count	Percentage	STRIDE Threats Category
Benign	Benign	Benign (Normal Traffic)	230,339	2.62%	-
Attack	Spoofing	ARP Spoofing	17,791	0.20%	Spoofing Identity (S)
	DoS	TCP Flood	462,480	5.27%	Denial of Service (D)
		UDP Flood	704,503	8.03%	
		SYN Flood	540,498	6.16%	
		ICMP Flood	514,724	5.87%	
	DDoS	TCP Amplification	987,063	11.25%	
		UDP Amplification	1,998,026	22.77%	
		SYN Flood	974,359	11.10%	
		ICMP Flood	1,887,175	21.51%	
	MQTT	Dos-Connect Flood	15,904	0.18%	
		Dos-Publish Flood	52,881	0.60%	
		DDos-Connect Flood	214,952	2.45%	
		DDos-Publish Flood	36,039	0.41%	
		Malformed Packets	6877	0.08%	
	Recon	Port Scanning	106,603	1.21%	Information Disclosure (I)
		OS Fingerprinting	20,666	0.24%	
		Ping_Sweep	926	0.01%	
		Vulnerability scanning	3207	0.04%	

3.1.2. Dataset Collection

Since the original version of the CICIoMT2024 dataset is given as CSV files (51 for train and 21 for test) of different sizes, we proceeded to combine them into two separate datasets, a training set with 7,160,831 traffic records and a test set with 1,614,182 traffic records, to ensure proper data split for model development. A 'label' column was automatically generated from each filename by removing a predefined suffix (e.g., "_train.csv") to preserve class information. The target column was then separated for supervised learning.

3.2. Proposed Model

HBiLD-IDS uses a synergistic combination of a Bidirectional Long Short-Term Memory layer with 128 units and a Deep Neural Network model with 128 to 64 ReLU units in a hierarchical processing pipeline that achieves superior analysis IoMT traffic.

The BiLSTM captures comprehensive bidirectional temporal patterns including subtle dependencies often overlooked in medical device communications, while the DNN transforms these sequential features into enhanced discriminative representations by parsing hierarchical features using nonlinear projection.

HBiLD-IDS demonstrates its ability to handle diverse IoMT communication protocols through its validation on the CIoMT2024 dataset. This comprehensive dataset includes network traffic from 25 real Wi-Fi and Bluetooth devices, along with 15 simulated devices using MQTT, protocols specifically chosen for their prevalence in healthcare. By training on this heterogeneous traffic, HBiLD-IDS effectively recognizes intrusions and anomalies regardless of the underlying protocol. It achieves this by prioritizing high-level behavioral signatures and traffic-derived features over rigid, protocol-specific rules, ensuring broad adaptability across various IoMT standards.

This BiLSTM-based approach tackles the absence of standardized security in the IoMT ecosystem by acting as a dynamic behavioral monitor. This method learns the unique "fingerprint" of normal healthcare devices activity, allowing it to detect and flag any deviations from established patterns. This adaptability makes it particularly effective for real-time intrusion detection within the heterogeneous and often inconsistent IoMT environment.

3.3. Data Preprocessing

The preprocessing pipeline for the dataset involved several critical steps to ensure high-quality input for machine learning models. First, after removing rows with excessive missing values and performing median imputation for numerical features, the nineteen target classes were one-hot encoded to eliminate ordinal bias. Second, a feature selection process sequentially applied the following: (1) a variance threshold to eliminate non-informative features, (2) correlation-based filtering to remove redundancy, and (3) RFE to select optimal features. Finally, Min–Max normalization (0–1 scaling) standardized feature ranges while preserving dataset-specific distributions, ensuring compatibility with diverse ML architectures. Both the train and test sets were subjected to all transformations in the preprocessing pipeline.

3.4. Data Splitting

We performed stratified splitting of the preprocessed training data into training (80%) and validation (20%) sets to ensure both model generalizability and reproducibility.

3.5. Model Architecture

The HBiLD-IDS architecture was designed around three fundamental principles: (1) temporal integrity preservation, (2) regularization robustness, and (3) training stability, implemented through the following technical components:

(a) Core Architecture:
- Temporal Processing: A 128-unit bidirectional LSTM layer (return sequences = True) maintains temporal resolution, with input features reshaped into 3D tensors (n_features $\times$ 1 $\times$ 1) for dimensional compatibility;
- Regularization Framework:
    - Immediate 40% variational dropout after BiLSTM layer;
    - Progressive dropout decay (40%$\rightarrow$30%) across subsequent distillation layers;
- Feature Distillation: Two dense layers (128$\rightarrow$64 neurons) with ReLU activation form the hierarchical feature extraction block;

(b) Optimization Configuration:
- Adam optimizer ($\eta = 5 \times 10^{-4}$ initial learning rate);
- Batch training (size = 128) for a maximum of 50 epochs;
- Tri-phase callback system:
    1. EarlyStopping: Patience = 20 epochs; $\delta = 0.001$ (prevents overfitting);
    2. ReduceLROnPlateau: Factor = 0.2 reduction; cooldown = 2 epochs (escapes local minima);
    3. ModelCheckpoint: Saves optimal weights based on validation performance3.6. Experimental Environnement.

3.6. Experimental Environnement

All experiments were conducted on a workstation with an Intel i5-12400F (6-core, 2.5 GHz), 32 GB RAM, and NVIDIA RTX 3060 Ti GPU (8 GB). The Python 3.10.7 implementation used Pandas for data processing and TensorFlow for model development, with evaluation metrics (accuracy, precision, recall, and F1-score) calculated via Scikit-learn.

3.7. Evaluation Metrics

The performance and effectiveness of our model are evaluated using standard evaluation metrics (accuracy, precision, recall, and F1-score), as well as the confusion matrix which is often used as evaluation metrics along with the four metrics with are calculated:

- True positives (TPs): Count of instances correctly predicted as positive.
- False positives (FPs): Count of instances wrongly predicted as positives.
- True positives (TNs): Count of instances correctly predicted as negatives.
- False positives (FNs): Count of instances wrongly predicted as negatives.

Accuracy: measures the proportion of correctly classified instances among all evaluation examples, obtained by dividing correct classifications by total classifications.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Precision: defined as the ratio of true positives to all instances predicted as positive, obtained by dividing number of true positives by the sum of number of true positives and number of false positives.

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Recall: measures the model's ability to correctly identify positive examples among all truly positive examples, obtained by dividing number of true positives by the sum of number of true positives and number of false negatives.

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

F1_score: The F1-score represents the harmonic mean of precision and recall, taking into account false alarms and missed detections.

$$F1\_score = 2\,\frac{(Precsion \times Recall)}{(Precsion + Recall)} \tag{4}$$

Confusion matrix: is a supervised learning evaluation tool that tabulates actual classes typically represented in rows versus predicted classes in columns across through four metrics: true positives (TPs), false positives (FPs), true negatives (TNs), and false negatives (FNs), enabling precise analysis of labels classification performance.

4. Results and Discussion

To develop an effective intrusion detection system for IoMT networks, we evaluated the performance of multiple models, including a Deep Neural Networks (DNNs) model, Hybrid CNN-DNN model, Hybrid LSTM-DNN model, and Hybrid BiLSTM-DNN (the proposed model).

The comparative results, as depicted in Figure 2, highlight the strengths and limitations of each approach across key metrics: accuracy, precision, recall and F1-score. The DNN model demonstrated strong performance in processing spatial data, achieving an accuracy of 97.54% (precision: 97.86%, recall: 97.54%, and F1-score: 97.30%). Its hierarchical feature extraction capability makes it well-suited for detecting patterns in structured network traffic. However, its inability to effectively analyze sequential or time-dependent data (a common characteristic of network intrusions) limited its overall effectiveness, particularly in dynamic IoMT environments.

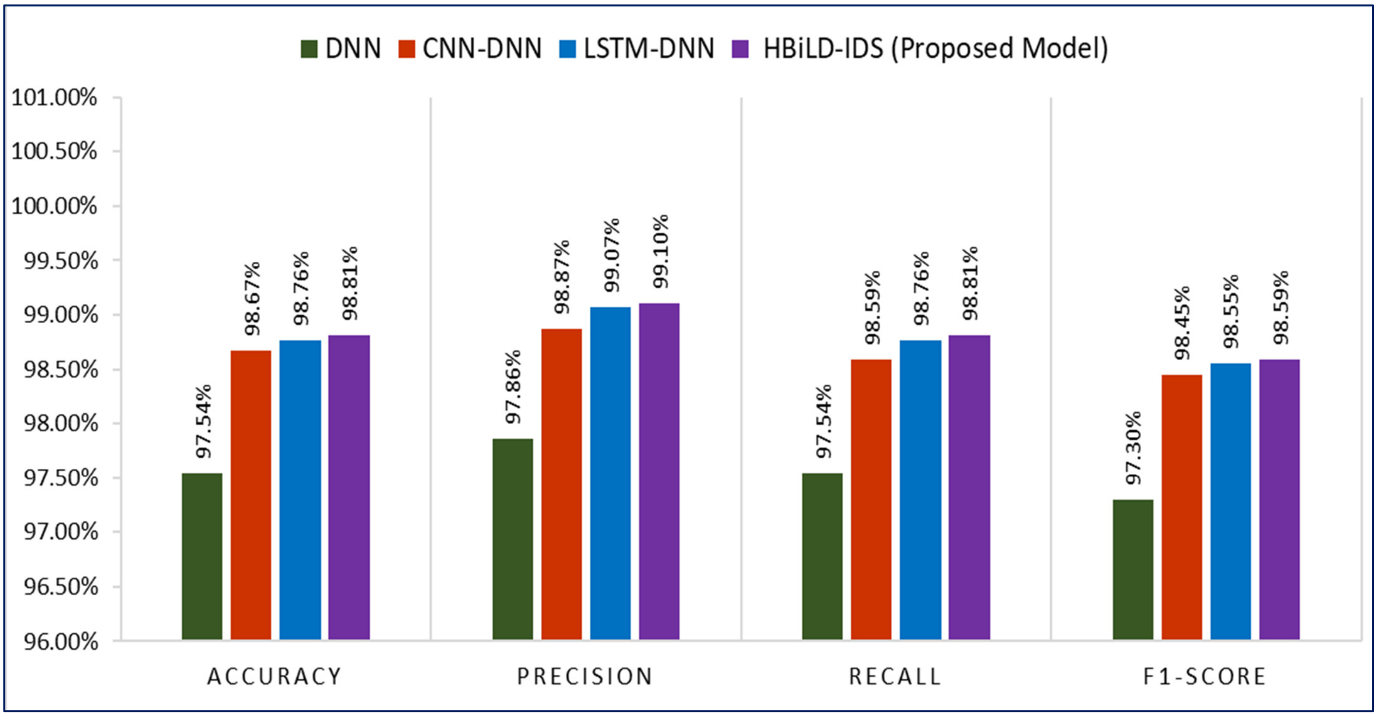

Figure 2. Model's performance metrics comparison.

While the CNN-DNN model can achieve strong performance (accuracy: 98.67%, precision: 98.87%, recall: 98.59%, and F1-score: 98.45%) by leveraging the CNN component for spatial feature extraction (e.g., identifying correlations among network attributes at a single point in time) and the DNN for subsequent classification, it inherently struggles with processing spatio-temporal features and capturing temporal dependencies. Therefore, the same limitation observed in plain DNNs regarding their inability to effectively analyze sequential or time-dependent data largely persists, hindering their overall effectiveness in dynamic IoMT environments where intrusions often manifest as evolving sequences of events.

To address this limitation, we integrated LSTM with DNN, leveraging LSTM's strength in capturing temporal dependencies in serial data. The resulting LSTM-DNN hybrid model showed significant improvement, achieving an accuracy of 98.76% (precision: 99.07%, recall: 98.76, and F1-score of 98.55%). This enhancement underscores the importance of combining spatial and temporal feature extraction for intrusion detection.

Further optimization was achieved by replacing the standard LSTM with a BiLSTM model which processes data in both forward and backward directions, enabling deeper contextual analysis to provide a comprehensive contextual understanding of network traffic. This is crucial for detecting sophisticated, multi-stage attacks and ensuring robustness across various attack scenarios. Following this, the DNN layers are vital for hierarchical feature extraction, learning abstract representations and complex nonlinear patterns, leading to powerful classification capabilities and scalability across different IoMT protocols. The proposed HBILD-IDS model, incorporating these advancements, outperformed all other models, attaining an accuracy of 98.81% (precision: 99.10%, recall: 98.81%, and F1-score of 98.59%).

Our proposed model demonstrates a significant reduction in false positives. As shown in Figures 3 and 4, HBiLD-IDS achieves perfect precision (100%) for nine (9) types of attacks (e.g.: TCP_IP-DDOS, TCP_IP-DOS, and MQTT_DDOS-Connect_Floods) and high precision between 86% and 99% for six (6) types (e.g.: MQTT-DDoS-Publish_Flood and Recon-Port_Scan). The remaining three types achieved precision ranging from 29% to 53% (Arp_Spoofing: 29%, Recon_Vul-Scan: 44%, and MQTT_DoS_Publish_Flood: 53%), performing better than DNN and CNN-DNN (Arp_Spoofing: 26%, Recon_Vul-Scan: 0%, and MQTT_DoS_Publish_Flood: 53%) for each one. This demonstrates its absolute reliability for countering widely represented threats, as well as rare threats, despite their under-representation in the data. Legitimate traffic was also accurately identified with a precision of 92%, enhancing its ability to distinguish between legitimate and malicious traffic types, effectively maintaining normal operations and limiting operational disruptions through threat filtering.

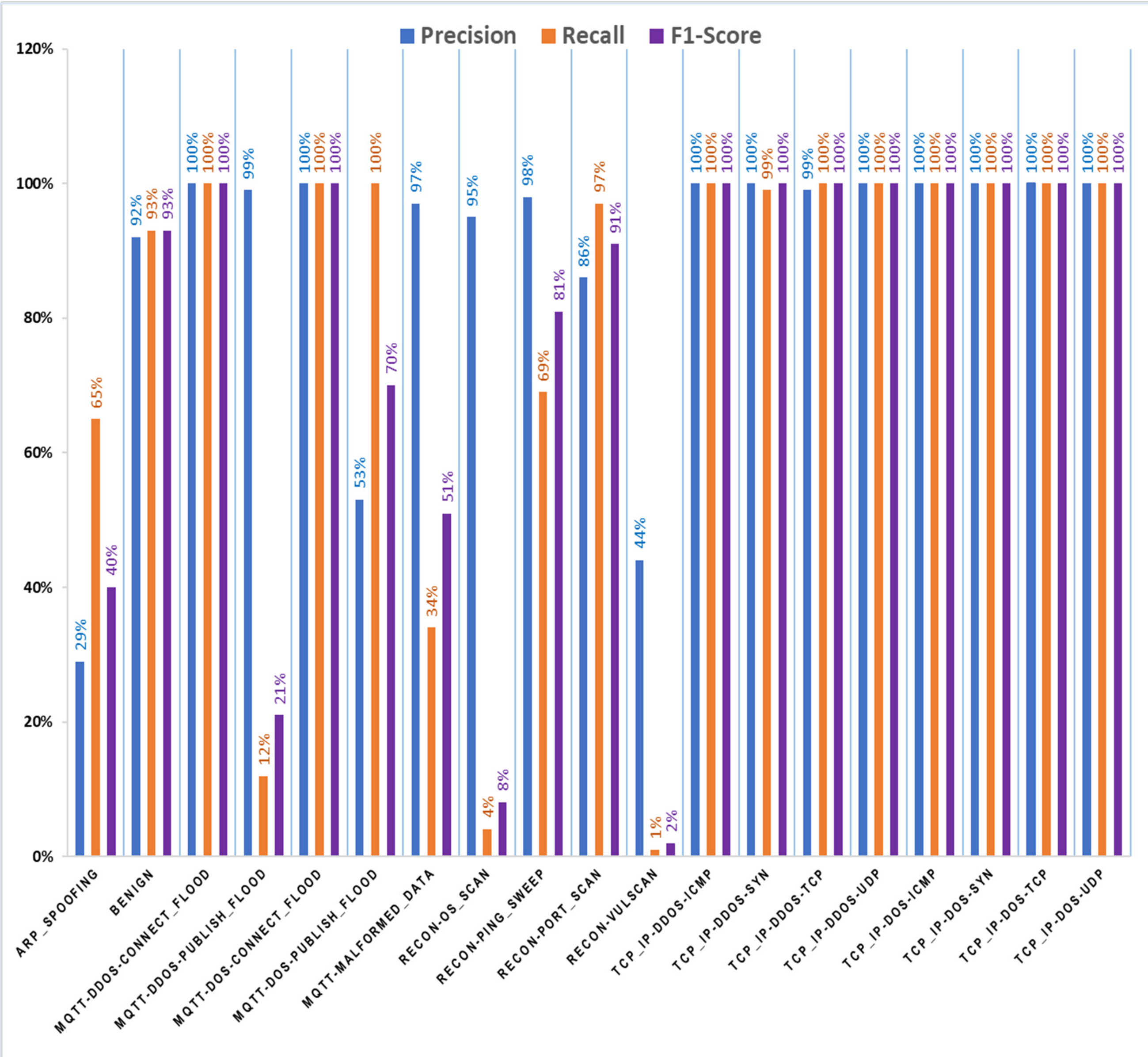

Figure 3. Per-class performance metrics comparison on the test set.

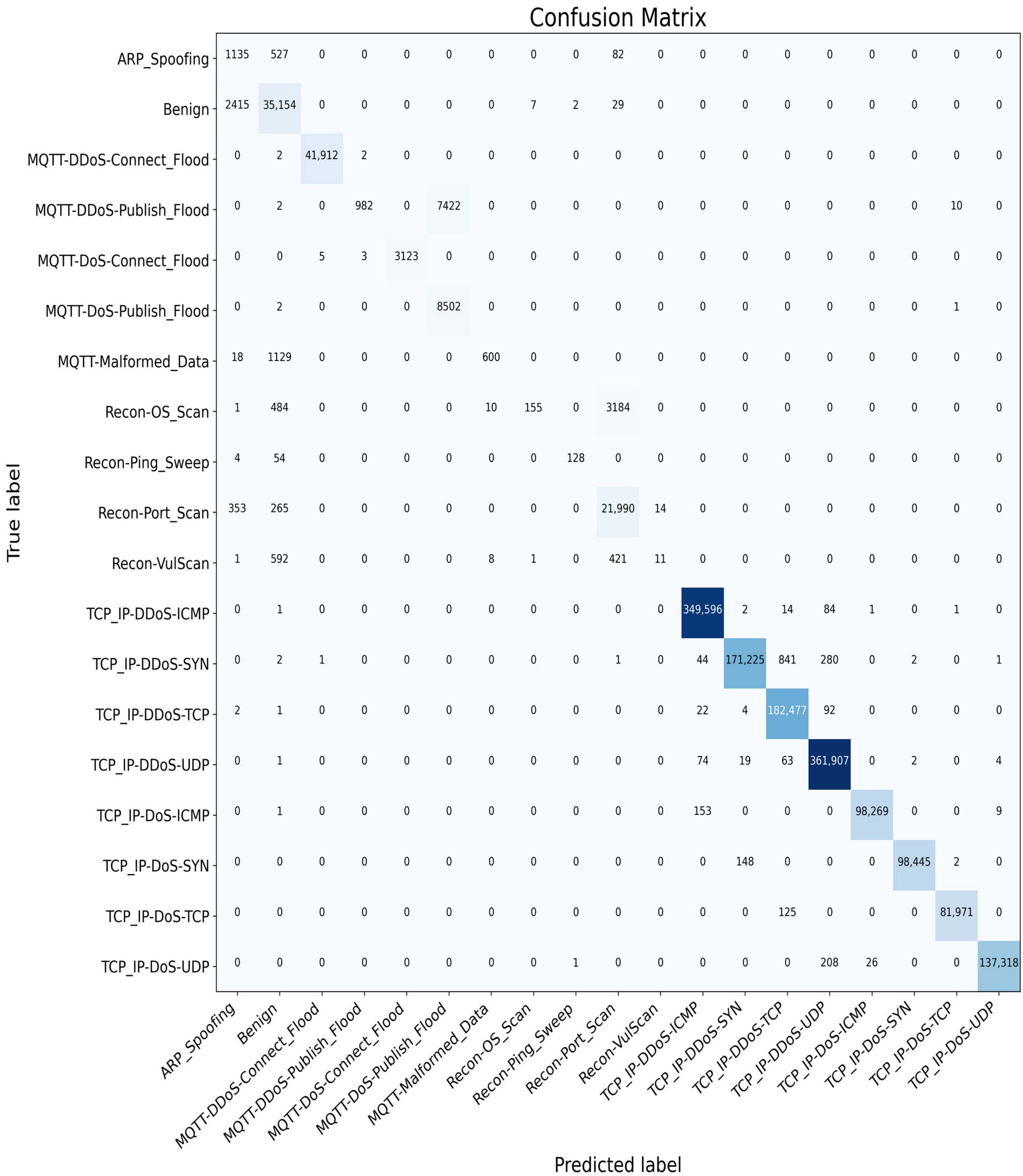

Figure 4. Nineteen-class confusion matrix evaluation of the proposed model on test data.

With high precision (99.10%), HBiLD-IDS confirms that identified attack attempts are mostly real attacks, mitigating false alarms. This robustness against imbalanced classes confirms the effectiveness of our approach in detecting both massive and rare threats but equally important attacks.

As shown in Table 3, HBiLD-IDS offers significant improvements over existing approaches in classifying 19 attacks on the CICIoMT2024 dataset, with outstanding performance (accuracy: 98.81%, precision: 99.10%, recall: 98.81%, and F1: 98.59%). It outperforms CNN-LSTM-RL by 21.08%, LSTM by 0.81%, and Random Forest by 25.51% in accuracy, while effectively reducing false positives and detecting various threats.

Table 3. Nineteen-class performance comparison of proposed model against previous works using CICIoMT2024 dataset.

Authors	ML/DL Technique	Accuracy	Precision	Recall	F1-Score
Shaikh et al. [18]	Hybrid (CNN-LSTM-RL)	0.7773	0.7602	0.7773	0.7247
Akar et al. [20]	LSTM	0.9800	0.9800	0.9800	0.9800
Dadkhah et al. [35]	RandomForest	0.7330	0.6910	0.5770	0.551
HBiLD-IDS (Proposed Model)	Hybrid (BiLSTM-DNN)	**0.9881**	**0.9910**	**0.9881**	**0.9859**

Conversely, Shaikh et al.'s hybrid CNN-LSTM-RL model [18], while adept at combining spatial feature extraction (CNN) with temporal modeling (LSTM), may inherently not excel at raw feature extraction and classification tasks that benefit from the bidirectional context captured by BiLSTM. The inclusion of reinforcement learning (RL) in such a hybrid model shifts its primary focus. The role of reinforcement learning is to optimize decision-making policies based on environmental interactions and rewards, rather than simply enhancing classification effectiveness. This fundamental difference in objectives can lead to lower classification performance metrics.

While Akar et al.'s LSTM model [20] shows strong performance in intrusion detection, HBiLD-IDS achieves superior results primarily due to its Bidirectional LSTM (BiLSTM) component. This bidirectional approach enables it to analyze temporal sequences by considering both preceding and succeeding data, a key advantage over unidirectional LSTMs that only look at past contexts. This comprehensive understanding, integrated with its hierarchical DNN structure, allows HBiLD-IDS to consistently outperform unidirectional LSTMs across all evaluation metrics.

Traditional machine learning algorithms, like Random Forest, despite their robustness in various applications, fundamentally rely on handcrafted features and decision tree structures. Unlike deep learning models, they cannot automatically learn complex, high-level features or critical temporal dependencies directly from raw data. This inherent limitation is starkly evident in the significantly lower performance metrics of Dadkhah et al.'s model [35] when using Random Forest, clearly demonstrating its inadequacy in handling the intricate and dynamic challenges of modern network intrusion detection compared to advanced deep learning approaches such as HBiLD-IDS.

By integrating complementary learning modes, the proposed hybrid approach achieves superior detection accuracy for both medical device threats and workflow anomalies compared to single-modality methods. The architecture establishes a new benchmark for scalable Internet of Medical Things (IoMT) security, with future enhancements targeting stealthy attack detection through improved training techniques.

Our approach demonstrates excellent performance, achieving high accuracy (86–100%) for 15 attack types and maintaining 92% accuracy on legitimate traffic. However, we have identified significant validity threats, primarily reduced accuracy (29% and 44%) for ARP spoofing and vulnerability scans, respectively. This indicates limitations in handling rare attack classes due to class imbalance and poor representation of minority attack characteristics. Given the major risks these specific attacks pose, we are actively addressing these limitations by expanding testing for rare attacks and improving imbalance mitigation in our ongoing research.

5. Conclusions

The Internet of Medical Things (IoMT) faces growing cyber security challenges due to its critical healthcare role and sensitive data, demanding robust intrusion detection systems (IDSs) tailored to medical environments. Our HBiLD-IDS model redefines the standards by combining sequential analysis (BiLSTM) and deep learning (DNN), achieving high performance on the CICIoMT2024 dataset: 98.81% accuracy, 99.10% precision, 98.81% recall, and 98.59% F1-score, outperforming existing solutions. These results prove its effectiveness in detecting dynamic attacks while minimizing false positives/negatives, an imperative to prevent serious medical errors. While ideal for real-world IoMT deployments, the widespread adoption of HBiLD-IDS will necessitate continuous innovations to effectively counter evolving cyber threats and further strengthen its resilience, particularly concerning the detection of rare and novel attacks. For future work, we specifically aim to enhance HBiLD-IDS to better address resource constraints within the IoMT ecosystem. This will involve leveraging a hybrid approach that integrates edge and fog computing for distributed processing and low-latency analysis. Furthermore, we intend to incorporate federated learning to enable privacy-preserving, collaborative model training, which can help in collectively identifying without compromising data privacy. This expanded framework is designed to ensure robust, real-time intrusion detection while simultaneously safeguarding sensitive medical data.

Author Contributions: Conceptualization: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug), M.H.; methodology: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug); software: H.B.; validation: M.M. (Mohammed Merzoug), M.M. (Mohammed M'hamedi), M.H., H.B., S.M.; formal analysis: H.B., M.M. (Mohammed M'hamedi), A.B., A.E.; investigation: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug), M.H., S.M.; resources: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug); data curation: H.B.; writing—original draft preparation: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug), M.H., A.E., S.M., A.B.; writing—review and editing: H.B., M.M. (Mohammed M'hamedi), M.M. (Mohammed Merzoug), M.H., A.E., S.M., A.B.; visualization: H.B.; supervision: M.M. (Mohammed Merzoug), M.M. (Mohammed M'hamedi), M.H., S.M.; project administration: M.M. (Mohammed Merzoug); funding acquisition: S.M., M.M. (Mohammed Merzoug). All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yin, U.; Zeng, Y.; Chen, X.; Fan, Y. The Internet of Things in Healthcare: An Overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
2. Aceto, G.; Persico, V.; Pescapé, A. The Role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges. *J. Netw. Comput. Appl.* **2018**, *107*, 125–154. [CrossRef]
3. El-Saleh, A.A.; Sheikh, A.M.; Albreem, M.A.M.; Honnurvali, M.S. The Internet of Medical Things (IoMT): Opportunities and Challenges. *Wirel. Netw.* **2025**, *31*, 327–344. [CrossRef]
4. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]

5. Villegas-Ch, W.; Govea, J.; Jaramillo-Alcazar, A. Tamper Detection in Industrial Sensors: An Approach Based on Anomaly Detection. *Sensors* **2023**, *23*, 8908. [CrossRef]
6. Tariq, U.; Ullah, I.; Yousuf Uddin, M.; Kwon, S.J. An Effective Self-Configurable Ransomware Prevention Technique for IoMT. *Sensors* **2022**, *22*, 8516. [CrossRef]
7. Alturki, B.; Abu Al-Haija, Q.; Alsemmeari, R.A.; Alsulami, A.; Alqahtani, A.; Alghamdi, B.M.; Bakhsh, S.T.; Shaikh, R.A. IoMT Landscape: Navigating Current Challenges and Pioneering Future Research Trends. *Discov. Appl. Sci.* **2025**, *7*, 26. [CrossRef]
8. Cao, Y.; Zhang, L.; Zhao, X.; Jin, K.; Chen, Z. An Intrusion Detection Method for Industrial Control System Based on Machine Learning. *Information* **2022**, *13*, 322. [CrossRef]
9. 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.* **2025**, *58*, 114. [CrossRef]
10. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. A Systematic Review of Data Protection and Privacy Preservation Schemes for Smart Grid Communications. *Sustain. Cities Soc.* **2018**, *38*, 806–835. [CrossRef]
11. Xiao, L.; Wan, Y.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
12. Yaacoub, J.-P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing Internet of Medical Things Systems: Limitations, Issues and Recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
13. Tsimpourlas, F.; Papadopoulos, L.; Bartsokas, A.; Soudris, D. A Design Space Exploration Framework for Convolutional Neural Networks Implemented on Edge Devices. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2018**, *37*, 2212–2221. [CrossRef]
14. Genuario, F.; Santoro, G.; Giliberti, M.; Bello, S.; Zazzera, E.; Impedovo, D. Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights. *Information* **2024**, *15*, 741. [CrossRef]
15. Yang, W.; Zhang, Y.; Chen, J.; Wang, L. An Industrial Network Intrusion Detection Algorithm Based on IGWO-GRU. *Cluster Comput.* **2024**, *27*, 7199–7217. [CrossRef]
16. Zhang, Y.; Liu, Y.; Guo, X.; Liu, Z.; Zhang, X.; Liang, K. A BiLSTM-Based DDoS Attack Detection Method for Edge Computing. *Energies* **2022**, *15*, 7882. [CrossRef]
17. Feng, W.; Tang, S.; Wang, S.; He, Y.; Chen, D.; Yang, Q.; Fu, S. Characterizing Perception Deep Learning Algorithms and Applications for Vehicular Edge Computing. *Algorithms* **2025**, *18*, 31. [CrossRef]
18. Shaikh, J.A.; Wang, C.; Sima, M.W.U.; Arshad, M.; Owais, M.; Hassan, D.S.M.; Alkanhel, R.; Muthanna, M.S.A. A Deep Reinforcement Learning-Based Robust Intrusion Detection System for Securing IoMT Healthcare Networks. *Front. Med.* **2025**, *12*, 1524286. [CrossRef]
19. Sharma, N.; Shambharkar, P.G. Multi-Attention DeepCRNN: An Efficient and Explainable Intrusion Detection Framework for Internet of Medical Things Environments. *Knowl. Inf. Syst.* **2025**, *67*, 5783–5849. [CrossRef]
20. 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**, *13*, 7002–7013. [CrossRef]
21. Naeem, H.; Alsirhani, A.; Alserhani, F.M.; Ullah, F.; Krejcar, O. Augmenting Internet of Medical Things Security: Deep Ensemble Integration and Methodological Fusion. *Comput. Model. Eng. Sci.* **2024**, *141*, 2185–2223. [CrossRef]
22. Tseng, S.M.; Wang, Y.Q.; Wang, Y.C. Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset. *Future Internet* **2024**, *16*, 284. [CrossRef]
23. Alsharaiah, M.A.; Almaiah, M.A.; Shehab, R.; Obeidat, M.; El-Qirem, F.A.; Aldhyani, T. An Explainable AI-Driven Transformer Model for Spoofing Attack Detection in Internet of Medical Things (IoMT) Networks. *Discov. Appl. Sci.* **2025**, *7*, 488. [CrossRef]
24. Faruqui, N.; Abu Yousuf, M.; Whaiduzzaman; Azad, A.; Alyami, S.A.; Liò, P.; Kabir, M.A.; Moni, M.A. SafetyMed: A Novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization. *Electronics* **2023**, *12*, 3541. [CrossRef]
25. Gueriani, A.; Kheddar, H.; Mazari, A.C. Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems. In Proceedings of the 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS), El Oued, Algeria, 24–25 April 2024; pp. 1–7. [CrossRef]
26. Sayegh, H.R.; Dong, W.; Al-Madani, A.M. Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data. *Appl. Sci.* **2024**, *14*, 479. [CrossRef]
27. Jony, A.I.; Arnob, A.K.B. A Long Short-Term Memory Based Approach for Detecting Cyber Attacks in IoT Using CIC-IoT-2023 Dataset. *J. Edge Comput.* **2024**, *3*, 28–42. [CrossRef]
28. Lipsa, S.; Dash, R.K.; Ivković, N. An Interpretable Dimensional Reduction Technique with an Explainable Model for Detecting Attacks in Internet of Medical Things Devices. *Sci. Rep.* **2025**, *15*, 8718. [CrossRef]
29. Talukder, M.A.; Islam, M.M.; Uddin, M.A.; Hasan, K.F.; Sharmin, S.; Alyami, S.A.; Moni, M.A. Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Data Using Oversampling, Stacking Feature Embedding, and Feature Extraction. *J. Big Data* **2024**, *11*, 33. [CrossRef]

30. Abbas, S.; Al Hejaili, A.; Sampedro, G.A.; Abisado, M.; Almadhor, A.S.; Shahzad, T.; Ouahada, K. A Novel Federated Edge Learning Approach for Detecting Cyberattacks in IoT Infrastructures. *IEEE Access* **2023**, *11*, 112189–112198. [CrossRef]
31. Doménech, J.; León, O.; Siddiqui, M.S.; Pegueroles, J. Evaluating and Enhancing Intrusion Detection Systems in IoMT: The Importance of Domain-Specific Datasets. *Internet Things* **2025**, *32*, 101631. [CrossRef]
32. Khanday, S.A.; Fatima, H.; Rakesh, N. A Novel Data Preprocessing Model for Lightweight Sensory IoT Intrusion Detection. *Int. J. Math. Eng. Manag. Sci.* **2024**, *9*, 188–204. [CrossRef]
33. Saran, N.; Kesswani, N. Intrusion Detection System for Internet of Medical Things Using GRU with Attention Mechanism-Based Hybrid Deep Learning Technique. *Jordanian J. Comput. Inf. Technol.* **2024**, *11*, 136–150. [CrossRef]
34. Anwar, R.W.; Abrar, M.; Salam, A.; Ullah, F. Federated Learning with LSTM for Intrusion Detection in IoT-Based Wireless Sensor Networks: A Multi-Dataset Analysis. *PeerJ Comput. Sci.* **2025**, *11*, e2751. [CrossRef]
35. Dadkhah, S.; Neto, E.C.P.; Ferreira, R.; Molokwu, R.C.; Sadeghi, S.; Ghorbani, A.A. CICIoMT2024: A Benchmark Dataset for Multi-Protocol Security Assessment in IoMT. *Internet Things* **2024**, *28*, 101351. [CrossRef]
36. Tany, N.S.; Suresh, S.; Sinha, D.N.; Shinde, C.; Stolojescu-Crisan, C.; Khondoker, R. Cybersecurity Comparison of Brain-Based Automotive Electrical and Electronic Architectures. *Information* **2022**, *13*, 518. [CrossRef]