Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Robust and Lightweight Intrusion Detection Framework for IoMT Networks with Cross-Domain Evaluation

Umair Maqsood
Taylor's University
NZ Jhanjhi
zamanj@sunway.edu.my
Sunway University
Fatima Iftikhar
Foundation University Islamabad
Raja Majid Mehmood
Multimedia University

Research Article

Keywords: Intrusion Detection System(IDS), Internet of Medical Things(IoMT), Cross-Domain Evaluation, Machine Learning, Logistic Regression

Posted Date: August 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10517817/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Robust and Lightweight Intrusion Detection Framework for IoMT Networks with Cross-Domain Evaluation

Umair Maqsood[1], NZ Jhanjhi[2,3*], Fatima Iftikhar[4], Raja Majid Mehmood[5,6*]

[1]School of Computer Science, Taylors University, Subang Jaya 47500, Malaysia.
[2]School of Computing and Artificial Intelligence, Faculty of Engineering and Technology, Sunway University, Bandar Sunway, Selangor Darul Ehsan, Malaysia.
[3]Office of Research and Development, Asia University, Taichung,Taiwan.
[4]Department of Engineering Technology, Foundation University Islamabad, Islamabad,Pakistan.
[5]Center for Advanced Analytics, COE for Artificial Intelligence, Multimedia University, Persiaran Multimedia, Cyberjaya 63100, Malaysia.
[6]Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia 63100, Cyberjaya, Selangor, Malaysia.

*Corresponding author(s). E-mail(s): zamanj@sunway.edu.my; rajamajid@mmu.edu.my;
Contributing authors: umairmaqsood089@gmail.com; fatima.iftikhar@fui.edu.pk;

Abstract

The rapid growth of the Internet of Medical Things (IoMT) has transformed the healthcare sector through connectivity, real-time functionality, and intelligence in medical examination practices, but it has introduced new challenges in cybersecurity, especially in intrusion detection in diverse and dynamic environments. This study proposes an IoMT-centered intrusion detection framework based on CICIoMT2024 as the main dataset, CICIoT2023 for cross-domain transfer, and Edge-IIoTset for external validity. Three Machine Learning (ML) Models, including Logistic Regression (LR), XGBoost, and Random Forest (RF) were trained and evaluated in the same-domain and cross-domain environments with additional threshold analysis. The findings reveal that XGBoost performed best on same-domain data, with 98.68% accuracy and 0.993 F1-score, and Random Forest achieved 98.07% accuracy, confirming the effectiveness of ensemble models for IoMT-specific data. In cross-domain environments, the proposed framework showed promising transfer performance, with Logistic Regression achieving 89.65% external accuracy and maintaining stable detection of the benign class, while under domain shift, ensemble models showed a performance degradation. The overall results indicate that effective cross-domain intrusion detection is achievable and possible with careful model selection and evaluation techniques. In addition, Edge-IIoTset could not be directly incorporated into transfer experiments due to incompatible feature schemas, highlighting challenges in cross-dataset compatibility. These results show that achieving only high same-domain accuracy is not enough for IoMT intrusion detection; rather, cross-domain stability, balanced detection, and compatibility with diverse datasets must be considered when deploying IDS in real-world healthcare environments.

Keywords: Intrusion Detection System(IDS), Internet of Medical Things(IoMT), Cross-Domain Evaluation, Machine Learning, Logistic Regression.

1 Introduction

The Internet of Things (IoT) has greatly transformed many industries, including healthcare and agriculture [1, 2]. Healthcare is defined as the practice of managing and improving well-being through

proper diet and exercise, as well as identifying and treating diseases and injuries to protect them from worsening [3]. The Internet of Medical Things (IoMT), part of a broader IoT, has gained potential to minimize the burden of healthcare systems using remote surveillance, patient tracking, and the real-time analysis of patient data. In modern medical systems, it is now considered an important technology [4, 5].

IoMT as shown in Figure 1, is a key branch of IoT emphasizing healthcare as a fundamental human need with expected revenue generating seven billion dollars [6, 7] covers multiple parts such as devices and sensors for collecting biomedical data, ranging from basic body sensors to advanced surgical equipment, enabling secure communication networks between medical personnel, patients and healthcare facilities also distributed IT infrastructures for building, accessing, and managing electronic health records [8] and healthcare-focused services and interactive design for patient care [9, 10].

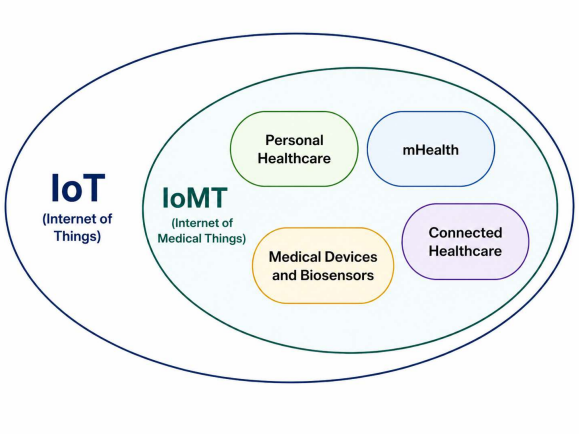


Fig. 1 IoMT as a healthcare-oriented subset of IoT.

1.1 Background & Motivation

The IoMT is innovating healthcare by integrating medical devices with cloud infrastructure and real-time data analysis to improve diagnostics and patient care [11–14], and within healthcare systems by utilizing wired, wireless, or hybrid communication networks to allow medical devices to exchange information smoothly and work together [15, 16]. Moreover, through personalized, predictive, and preventive medical techniques, IoMT contributes to enhanced patient outcomes and overall health, and its combination with big data analytics enables more informed and efficient decision-making in healthcare [17].

One of the most remarkable uses of IoMT is in telemedicine, where patients can get healthcare services remotely using mobile or virtual platforms, giving support for people living in isolated or low-resource locations [18]. Figure 2 illustrates the interconnected framework of IoMT, describing how smart devices work together to provide smooth and timely patient care.

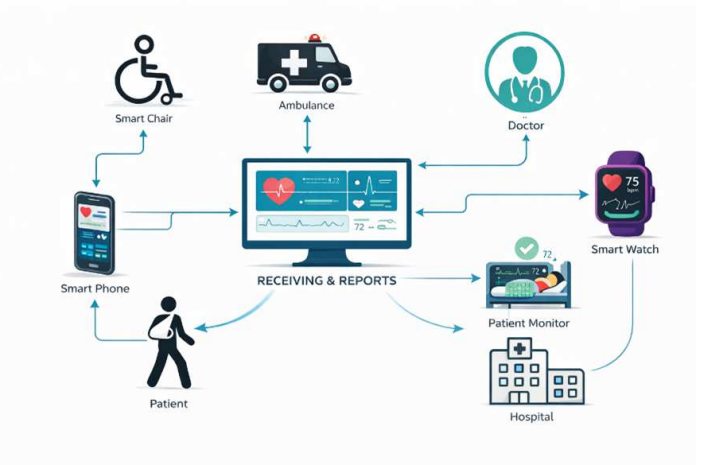


Fig. 2 Framework of IoMT.

In a current study, ENISA, a European Union agency, highlighted that during 2023, especially in the healthcare sector there was a rise of 55% in cybersecurity attacks, with the devices like IoMT being major targets [19] and weaknesses of these devices create major risks to data privacy and safety of patient, prioritizing security of IoMT in emerging cybersecurity frameworks [20]. Another recent report, according to CrowdStrike global threat [21], highlights that in 2025, a total of 9% of global intrusion attacks targeted healthcare systems however, to reduce these attacks in IoMT environments, Intrusion Detection Systems (IDS) are globally used nowadays [22], while in real time these systems detect attacks, analyze security threats, and monitor network traffic.

Intrusion Detection Systems (IDSs) are defined as autonomous hardware or software solutions that are created to detect and respond to cyber threats and play a critical role in analyzing advanced attacks that traditional security systems may often fail to detect [23]. Through data analysis, some AI-based IDS that specifically utilize machine learning (ML) are becoming an important technology for detecting cyber-attacks, and IoT applications such as mobile computing and agriculture use ML widely [24, 25]. Despite this progress in ML based security frameworks, some challenges remain, such as maintaining interpretability, efficiency, accuracy, and changing threat landscapes [26, 27].

In security-sensitive environments, balancing false positives and negatives remains a major challenge. The integration of ML models with IDS describes a novel technique that reduced detection time, and improved detection accuracy as compare to traditional methods [28] while recent studies [29, 30] highlights that the present AI based IDS are not well optimized for real world IoMT environments leading to biased and unreliable detection results also many current IDS are specifically designed and developed for general IoT environments failing to analyze the requirements and security challenges of IoMT environments [31–34]. This weakness is mainly due to depending upon the general IoT datasets, which do not track and analyze IoMT-specific attacks, making them less reliable for environments that are specifically for healthcare.

1.2 Cybersecurity Challenges in IoMT

Cyber threats in IoMT devices and poorly implemented encryption protocols increase the risk of unauthorized access to important patient information. The unauthorized access to the medical records of patients with a very weak authentication system emphasizes the need for strong security [35, 36], while Figure 3 illustrates some security challenges in the IoMT environment.

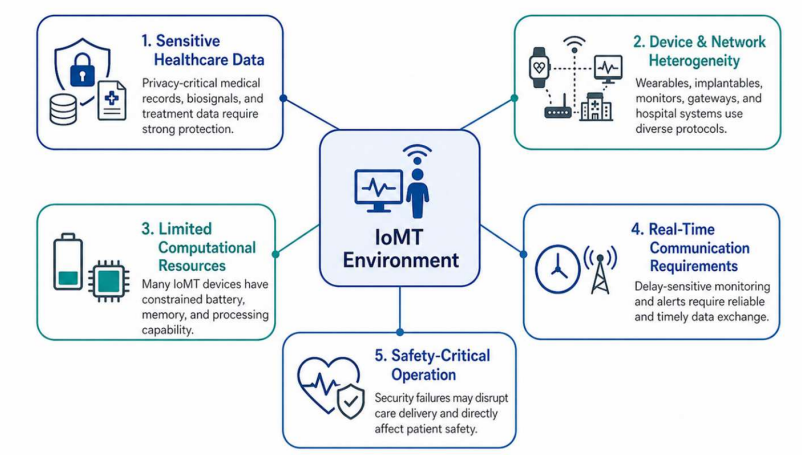


Fig. 3 Security challenges in IoMT conditions.

In developing countries, issues of privacy and security in IoMT systems always remain a crucial barrier, while serious challenges arise from unauthorized use and sharing of medical data, the possibility of re-identifying anonymized data, and difficulties in managing data accuracy represent huge challenges in healthcare systems [37, 38]. Table 1 describes the important challenges of security in IoMT environments.

Table 1 Security constraints in IoMT

Security Challenge	Description	Impact on IoMT Systems
Sensitive healthcare data [39]	IoMT devices process medical records, biosignals, telemetry, and treatment information.	Data breaches or tampering may affect privacy, diagnosis, and patient care.
Limited computational resources [39]	Many IoMT devices have constrained battery, memory, and processing capacity.	Lightweight and efficient security mechanisms are required.
Device and network heterogeneity [40]	IoMT environments include wearables, implantables, bedside monitors, gateways, and hospital systems using different protocols.	Heterogeneity complicates standardization, security management, and intrusion detection.
Safety-critical operation [40]	IoMT systems support healthcare services where interruptions may affect patient safety.	Security measures must preserve both protection and clinical continuity.
Real-time communication requirements [41]	IoMT applications rely on timely monitoring, alerting, and data exchange.	Delays or service disruption may directly affect medical response and treatment.

1.3 Limitations of Existing Intrusion Detection Systems

Machine learning and deep learning-based IDS have shown great performance, but multiple challenges still limit their effective deployment. Table 2 illustrates some major key challenges in IoMT environments.

With these limitations in Table 2, the study aims to address the key challenges through an IoMT-centered evaluation framework. Three ML models, Random Forest (RF), XGBoost, and Logistic Regression (LR), were used to analyze both ensemble and linear-based learning behavior. The design includes feature reduction and crash-safe sampling to improve computational performance and class-sensitive testing to assess domain shift. This design allows for a more realistic evaluation of the robustness, efficiency, and generalizability of intrusion detection systems in IoMT systems.

The paper is organized as follows: Section 2 reviews the related work on intrusion detection in IoMT and IoT conditions; Section 3 presents the methodology, whereas Section 4 discusses the results under both the same-domain and cross-domain environments. Section 5 describes the conclusion & outlines the future work directions.

Table 2 Limitations of Existing ML/DL Based IDS

Limitation	Description	Practical Implication
High false positives / benign-class misclassification	Normal traffic may be classified as malicious [42–44].	Increases false alarms and analyst burden; balancing sensitivity and precision remains difficult [45].
High computational cost	DL models such as CNNs and RNNs require high computational resources and long training time [44, 46, 47].	Limits deployment in constrained IoT/IoMT devices; lightweight alternatives still need improvement [48, 49].
Weak cross-domain generalization	Models may not remain reliable when transferred across datasets or environments [46, 50].	High in-domain accuracy may not guarantee robust external performance.
Class imbalance and minority-class degradation	Imbalanced IDS datasets can weaken minority-class detection [39, 50].	Class-sensitive evaluation is required because overall accuracy may become misleading.
Dataset compatibility/schema mismatch	Different datasets may use incompatible feature spaces [44, 51, 52].	Direct transfer may require feature harmonization or schema alignment.

2 Related Work

In this study, authors [53] investigated whether general IoT datasets can be used for an intrusion detection system in IoMT, so they compared CICIoT2023 with CICIoMT2024 and found that when applied to different datasets, such as training on one model and testing on another, models do not perform well. In many cases, the F1-score decreases, indicating that simple IoT data does not fully match IoMT data. The authors also highlighted issues in CICIoMT2024, such as improper data splitting, time-related issues, and imbalanced datasets; additionally, by using preprocessing approaches such as proper dataset partitioning, uniform windowing, and balanced data, they significantly improved results.

To detect cyberattacks in IoMT traffic, the authors proposed [54] a Tsetlin machine-based IDS using the CICIoMT2024 dataset and the key benefit of this approach is its transparency, as the model describes its decision by using visualization techniques, class vote scores, and logical rules. In binary classification, they achieved an accuracy of 99.5% while in multi-class classification, they achieved an accuracy of 90.7%. This study also highlighted that the traditional IDS techniques face challenges with large traffic volume and new attacks, while this proposed model gives an interpretable and lightweight alternative.

A capsule neural network (CapsNet) based adaptive IDS for IoMT was presented [55], and the authors' goal was to analyze both known and unknown attacks while decreasing false positives and negatives. They also explained that the traditional signature-based IDS cannot control new threats, while in network traffic, many ML techniques may miss typical relationships. CapsNet was utilized in this study because of its ability to model spatial and hierarchical relationships in data. They achieved strong performance and got an accuracy of 98.37% with precision 98.57%, recall 98.17%, and F1-score 98.37%. The findings demonstrate that this technique is more suitable and reliable for controlling dynamic IoMT attack scenarios.

A deep learning-based technique for multi class IDS in IoMT was presented [56] using the CICIoMT2024 dataset; however, across multiple classification scenarios, the authors compared a conventional DNN model with a hybrid GRU-DNN model, including 2-class, 6-class, and 19-class tasks related to intrusion detection. They also highlighted that previous studies focused only on binary classification, while this study addressed the need for realistic multi class detection. The dataset consists of traffic from 40 IoMT devices and 18 different types of attack across Bluetooth, MQTT, and WiFi, and after applying preprocessing approaches including scaling, encoding, and feature selection, they achieved an accuracy of 98.4% and an F1 score of 98.2% in the 19-class scenario.

HIDS-IoMT hybrid deep learning-based IDS system was presented [57], and the authors combined CNN and LSTM networks. In this technique, they used CNN for feature extraction and LSTM for capturing patterns in network traffic data, and the model was deployed on a Raspberry Pi within a fog computing architecture, enabling decentralized detection and low latency closer to IoMT devices. The system was evaluated using Edge-IIoTset and IoTID20 datasets, which consist of real-world attacks such as HTTP, UDP, SYN flood, SQL injection, and scanning attacks. They achieved an accuracy of 99.2%, precision 99.1%, recall 99.99%, and an F1-score of 99.95%, and they also highlighted that for real-time IDS in IoMT environments, integrating deep learning with fog computing is very suitable.

A framework for intrusion detection was presented [58] that at the same time balances interpretability, accuracy, and computational efficiency, while the authors utilized the XGBoost model and compared it with Logistic Regression and applied SHAP (Shapley Additive explanations) to describe feature importance. They introduced a late fusion technique based on max voting. XGBoost gives strong recall and accuracy of 0.97, whereas the fusion model reduces false negatives, enhances fusion, and achieves precision of 0.98. Furthermore, the study highlighted that IDS models can be both explainable and effective while managing computational efficiency.

Another study [59] presented a complete intrusion detection framework for IoMT which covers both design and real-world deployment. Using an IoMT testbed, they implemented a hybrid anomaly-based IDS on low-power devices such as Raspberry Pi. Unlike traditional approaches, they used novelty and outlier detection methods to analyze both known and unknown attacks, and by using testbed, they generated a new dataset due to the absence of reliable existing data. Before deployment, multiple algorithms, including isolation forest, LOF, MCD, and OCSVM, were evaluated. With very low computational cost, the system achieved strong detection performance, requiring less than one percent of CPU usage.

Table 3 Comparative Analysis of Intrusion Detection in IoMT/IoT.

Paper	Methods Used	Algorithms	Accuracy / Performance	Limitations
[53]	Cross-domain comparison of IoT and IoMT datasets	ML-based IDS models	Performance improved after preprocessing; cross-domain F1 dropped in some cases	Generic IoT datasets may not represent IoMT traffic well.
[54]	Explainable IDS using rule-based learning	Tsetlin Machine	99.5% binary accuracy; 90.7% multi-class accuracy	Lower multi-class performance; needs real-world validation
[55]	Adaptive deep learning IDS	CapsNet	98.37% accuracy	Computational cost; limited deployment testing
[56]	Multi-class IoMT intrusion detection	DNN, GRU-DNN	GRU-DNN: 98.4% accuracy; 98.2% F1-score	Needs more computational resources; results depend on data quality
[57]	Fog-based hybrid IDS	CNN-LSTM	99.92% accuracy; 99.95% F1-score	Needs validation on more IoMT datasets
[58]	Explainable and cost-aware IDS	XGBoost, Logistic Regression, Fusion	XGBoost: 0.97 accuracy; Fusion: 0.98 precision	False negatives and cost remain important
[59]	Anomaly-based IDS with testbed dataset	OCSVM, LOF, KDE, MCD, Isolation Forest	Strong detection; below 1% CPU usage	Evaluation is limited to a specific testbed environment

Existing studies in Table 3 have achieved high detection performance using ensemble-based or deep learning models, but these techniques are tested on single datasets and need higher computational resources. Moreover, through cross-validation and cross-domain testing between both IoMT and IoT datasets, there is still limited work on lightweight machine learning models. So, to overcome these limitations, this study aims to develop an efficient and lightweight intrusion detection system framework reliable for practical IoMT environments.

3 Methodology

3.1 Study Design

The main objective of this study was to evaluate Intrusion Detection in IoMT systems under both the same domain and cross-domain environments using a single dataset. The main goal was whether the models trained on IoMT data can maintain their effectiveness when applied to other IoT environments while also maintaining their accuracy. In order to achieve this objective, CICIoMT2024 was selected as the main dataset because it is specifically for IoMT attack and traffic scenarios, and for cross-domain validation, CICIoT2023 was used. To evaluate robustness, Edge-IIOTset was also examined as an additional dataset because of its feature incompatibility with CICIoMT2024; it was not fully integrated into the environment. Furthermore, in addition to accuracy, precision, recall, and F1-score,

the paper also reports inference time, memory consumption, and the number of selected features to assess the model's suitability to the resource-constrained IoMT environment.

3.2 Experimental Framework

The overall methodology consists of five main stages: acquisition of the dataset, preprocessing of data, feature selection, model development, and evaluation. This structure was chosen to ensure that the study will focus not only on classification performance but also on the transferability and model suitability under diverse conditions. In IoMT/IoT environments, Figure 4 illustrates the overall workflow of the study under same-domain and cross-domain settings, from data selection and preprocessing, through model building, evaluation under four different experimental scenarios, and final binary classification and performance evaluation.

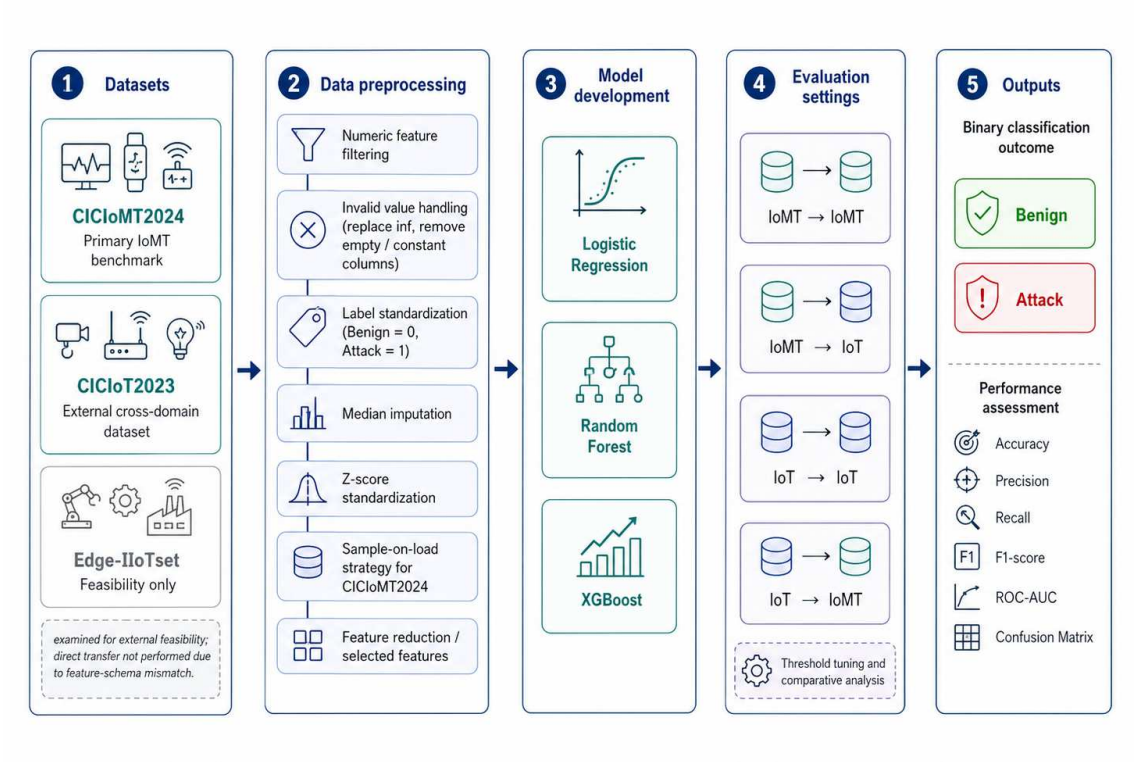


Fig. 4 Experimental Framework across all datasets

3.3 Datasets and their roles in the experiment

In this study, three datasets were utilized. For training and same-domain evaluation, CICIoMT2024 [60] was used as a primary dataset, because the objective was to examine intrusion detection specifically in IoMT environments instead of IoT environments. While CICIoT2023 [61] was utilized as an external dataset to evaluate cross-domain performance and for robustness evaluation, Edge-IIoTset [62] was explored as an additional dataset; however, even after normalization attempts, its features are not compatible with the CICIoMT2024 dataset. So, Edge-IIoTset was not included and was used only to assess methodological feasibility. The three datasets and their roles are described in Table 4.

Table 4 Datasets used and their roles

Dataset	Role in Study	Relevance	Limitation
CICIoMT2024	Primary training and testing dataset	IoMT-specific benchmark with medical-device traffic	Strong class imbalance
CICIoT2023	Cross-domain comparison dataset	Suitable for transfer evaluation between IoMT and generic IoT	Not healthcare-specific
Edge-IIoTset	Additional robustness candidate	Heterogeneous IoT/IIoT environment	Direct transfer infeasible due to schema incompatibility

3.4 Data Preprocessing & their Steps

A preprocessing pipeline was established before training the models. The success of intrusion detection relies heavily on dataset size and data quality, so preprocessing was not considered a technical, but a crucial, step in the process. Preprocessing steps consist of selection of numeric features, correction of invalid values, elimination of noise features, imputation, scaling, and feature selection.

3.4.1 Cleaning of data

First, the datasets were filtered to include only numeric features that can be used for machine learning. Infinite values were changed to missing values. The missing values were imputed with the median values. This eliminated training instability and bias in the machine learning model caused by invalid numeric representations.

3.4.2 Labels Standardization

In CICIoMT2024, any files containing Benign were labelled as benign, and all others were labelled as attack using binary labelling. In CICIoT2023, labels were based on the choice of folders in the sampled experiments. For Edge-IIoTset, the tentative mapping of Normal traffic to benign and Attack traffic to attack was possible at the label level, but not transferable because the feature schema was not common.

3.4.3 Imputation and Standardization

Following imputation, all remaining features were z-score standardized to have a similar scale. This was important as the candidate features had vastly different ranges and magnitudes, and it was essential that the features had a common scale to allow comparison of models.

3.4.4 Sampling Technique

CICIoMT2024 is large-scale and, when loading the raw training and testing partitions, memory failures occurred during experimentation. To resolve this, the sample-on-load technique was used. Rather than loading the entire dataset and sampling, smaller subsets were sampled during loading. This allowed for lower memory consumption without sacrificing diversity of attack files and benign samples. The resulting crash-safe IoMT-centered experiments preserved class diversity and were manageable. The steps, operations, and purpose of the data preprocessing pipeline are shown in Table 5.

Table 5 Preprocessing pipeline of data

Step	Operation	Purpose
1	Numeric feature filtering	Remove incompatible variables
2	Replace inf / $-$inf with NaN	Stabilize model training
3	Remove all-NaN and constant columns	Eliminate non-informative features
4	Median imputation	Handle missing values
5	Standardization	Normalize feature scale
6	Crash-safe sampling	Reduce memory load and preserve feasibility

3.5 Feature Selection Approaches

Feature selection was used to increase efficiency, control feature dimensionality, and manage discriminative potential. Instead of using the full set of features, this study used Select K Best with mutual information to select the top subset of features following preprocessing. This approach was preferred as it was efficient, model-independent, and suitable for both linear and tree-based models.

In the crash-safe IoMT-centered experiments, the resulting representation consisted of 15 features, which were enough to maintain high same-domain discrimination while being computationally efficient. The number of features was thus not only reduced to save memory, but also it is well aligned with the study's lightweight methodological aim. The stages, methods, and their role in the feature selection are described in Table 6.

Table 6 Feature Selection Technique

Stage	Method	Role
Stage 1	Numeric filtering and constant-column removal	Eliminate unusable or non-informative variables
Stage 2	SelectKBest with mutual information	Retain the most predictive features

3.6 Development of Models

The study compared the results obtained from three ML algorithms: Logistic Regression, Random Forest, and XGBoost. Logistic Regression was used as a linear baseline, Random Forest as a strong ensemble baseline, and XGBoost as the primary boosting-based classifier, as described in Table 7. Comparing the performance of linear, bagging, and boosting-based classifiers allows the investigation of whether observed transfer behavior is specific to the model or consistent across different families of learners.

Table 7 ML models

Model	Type	Role
Logistic Regression	Linear classifier	Interpretable baseline
Random Forest	Tree ensemble	Nonlinear baseline
XGBoost	Gradient boosting	Main high-performance classifier

3.7 Experimental Scenarios across Same and Cross-Domain

Model evaluation were conducted under five different experimental scenarios,

1. **IoMT to IoMT:** To establish a main-domain IoMT baseline, training and testing were conducted using the CICIoMT2024 dataset.
2. **IoMT to IoT:** To examine a cross-domain transfer from medical to IoT traffic, training was conducted on CICIoMT2024 and testing was conducted on the CICIoT2023 dataset.
3. **IoT to IoT:** To establish a main in-domain IoT baseline, training and testing were conducted using the CICIoT2023 dataset
4. **IoT to IoMT:** To examine a reverse direction transfer, training was conducted on the CICIoT2023 dataset and testing was conducted on the CICIoMT2024 dataset.
5. **IoMT to Edge-IIoTset:**Edge-IIOTset was also examined as an additional dataset to evaluate robustness, but because its features were not fully compatible with CICIoMT2024, it was not fully integrated into the environment.

The threshold tuning showed only minor improvement in XGBoost cross-domain performance, indicating that degradation was mainly due to dataset domain shift rather than an unsuitable default threshold.

3.8 Performance Evaluation Metrics

Performance was evaluated using accuracy, precision, recall, F1-score, ROC-AUC, and confusion matrices as shown in Table 8. Accuracy was included as a general metric but it was not considered to be sufficient due to class imbalance and attack-dominant predictions. As a result, class-wise performance, particularly benign-class precision, recall, and F1-score, were focused on in the transfer experiments. Training time and inference time were also measured to enable efficiency analysis. The study uses accuracy [63], precision [64], recall [65] and F1-score [66] metrics to measure classification performance as follows in the equation 1, 2, 3, 4:

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

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

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

$$\text{F1-score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

where TP, TN, FP, and FN are true positive, true negative, false positive, and false negative, respectively. For this study, true positives, true negatives, false positives, and false negatives are defined as detected attacks, detected benign, false alarms, and missed attacks, respectively. While accuracy was reported as overall performance, precision, recall, F1-score, and confusion matrix were of particular interest because class-specific behavior, particularly degradation in the benign class, was a key focus of cross-domain evaluation.

Table 8 Evaluation Metrics

Metric	**Purpose**
Accuracy	Overall correctness
Precision	False-alarm control
Recall	Detection sensitivity
F1-score	Balance between precision and recall
ROC-AUC	Probability-ranking performance
Confusion matrix	Class-specific error analysis
Training time	Offline computational cost
Inference time	Online efficiency

3.9 Explainability Shape Based Strategy

Explainability was introduced as a valuable step of the proposed framework using the SHAP (SHapley Additive exPlanations) framework to explain the best tree-based model selected in the IoMT experiments. The purpose of this step is to determine the contribution of each feature in the model's predictions. The explainability analysis includes:

1. Overall feature importance, to rank the features that have the biggest influence on the model
2. SHAP summary plots, to display feature effects on all instances
3. Dependence plots, to understand feature effects
4. Local explanations, to examine individual benign and attack samples

This component adds transparency and helps to build trust in the intrusion detection system, which is particularly important in the health sector where decisions of models need to be accurate as well as understandable.

3.10 Threshold Tuning Analysis

Threshold tuning was applied for cross-domain predictions using XGBoost to see whether the transfer degradation could be mitigated by adjusting the threshold. Many threshold values were tested, and macro-F1, balanced accuracy, and class-specific metrics were recorded. This step was added to rule out two possibilities: transfer degradation due to a mismatch in thresholds; and transfer degradation due to domain shift. From the results, it was clear that changing the threshold provided only marginal improvements, suggesting the primary cause of degradation was a distribution shift between the datasets, rather than an inappropriate default threshold.

3.11 Technical overview of Edge-IIoTset

In this study, we considered Edge-IIoTset as an external robustness benchmark. But a detailed inspection of the schema showed that the feature overlap between CICIoMT2024 and Edge-IIoTset was zero. CICIoMT2024 had a schema with flow-statistical features, such as*header_ length*, rate, *tot_ sum*, variance, while Edge-IIoTset had packet and protocol-level features, such as *frame_ time*,

tcp_ dstport, *dns_ qry_ name*, and *mqtt_ topic*. As there was no common feature space between the two datasets, the transfer evaluation would have required additional feature engineering or schema harmonization; therefore, it was not included in the experiments.

4 Results

4.1 Overview of Experimental Results

This section presents the results of the chosen ML models in the same and cross-domains. We present the results in four experimental settings: IoMT to IoMT, IoMT to IoT, IoT to IoT, and IoT to IoMT. Further analyses are included for threshold adjustment and external data. In this section, we aim to not only determine the best-performing model in each scenario, but also to see if the ranking of the models is consistent across different training and testing domains.

The findings indicate that there is a clear difference between in-domain performance and cross-domain robustness. In in-domain testing, XGBoost consistently performed the best. But in cross-domain transfer tests, Logistic Regression and XGBoost showed more consistent and balanced performance, especially for the benign class. These findings show that in-domain effectiveness is not enough to provide practical robustness in different IoMT/IoT conditions.

4.2 Same-domain performance on CICIoMT2024 Dataset

In the first experiment, we tested three ML models in the IoMT-to-IoMT scenario, training and testing on the CICIoMT2024 dataset. This is the main within-distribution (in-domain) experiment for the study. In the crash-safe implementation of the experiment, the pre-processed feature matrices had 15 selected features, 118,113, and 53,280 sampled instances in the training and testing sets, respectively. The class distribution was heavily unbalanced towards attack, with 115,713 attack and 2,400 benign instances in the training data, and 50,423 attack and 2,857 benign instances in the testing data. Table 9 illustrates the IoMT-to-IoMT performance of three ML Models.

Table 9 IoMT to IoMT Performance

Model	**Accuracy**	**Precision**	**Recall**	**F1-score**	**ROC-AUC**	**Training Time (s)**
Logistic Regression	0.7253	0.9905	0.7166	0.8316	0.9225	4.10
Random Forest	0.9807	0.9954	0.9842	0.9898	0.9965	13.88
XGBoost	0.9868	0.9912	0.9948	0.9930	0.9959	4.59

XGBoost performed best on the IoMT to IoMT setting, with a test accuracy of 98.68%, test F1-score of 99.30%, and recall of 99.48%. Random Forest also delivered good performance (98.07% accuracy and 98.98% F1-score). Logistic Regression was much worse, with 72.53% accuracy and 83.16% F1-score. Figure 5 illustrates the training and testing accuracy of ML models in the IoMT-to-IoMT setting.

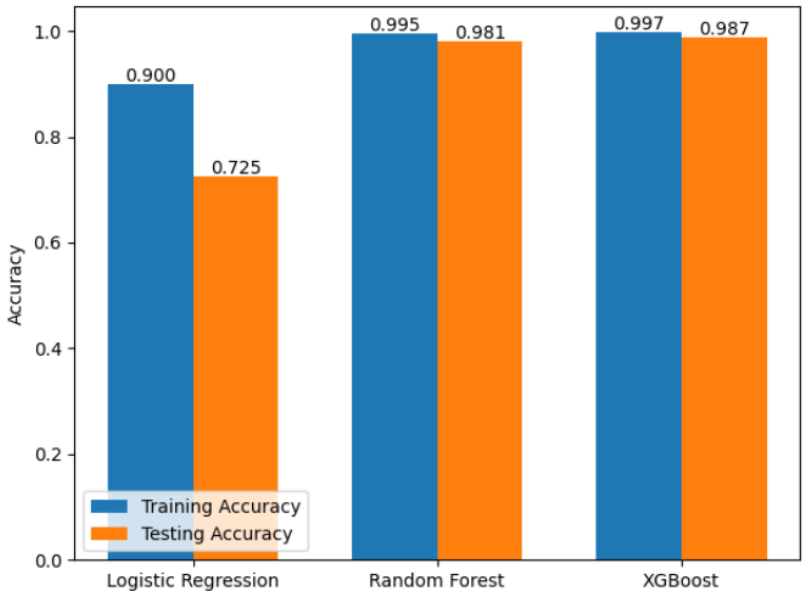


Fig. 5 IoMT to IoMT: Training vs Testing Accuracy

These predictions confirm that the main IoMT dataset is best served by a nonlinear ensemble model, rather than a linear decision boundary. This is also supported by the class-wise results as shown in Table 10. The benign-class F1-scores of XGBoost and Random Forest were 0.8725 and 0.8368, respectively. By contrast, Logistic Regression achieved a benign-class F1-score of just 0.2554, while achieving a benign recall of 0.8785. This suggests that Logistic Regression achieved benign sensitivity at the cost of misclassifying many attack samples, resulting in poor class balancing. Across both classes, Random Forest and XGBoost managed much better joint performance.

Table 10 Class-wise IoMT to IoMT results

Model	**Benign Precision**	**Benign Recall**	**Benign F1**	**Attack Precision**	**Attack Recall**	**Attack F1**
Logistic Regression	0.1494	0.8785	0.2554	0.9905	0.7166	0.8316
Random Forest	0.7670	0.9205	0.8368	0.9954	0.9842	0.9898
XGBoost	0.9024	0.8446	0.8725	0.9912	0.9948	0.9930

Thus, the same-domain IoMT experiment suggests XGBoost is the best in-domain model, with Random Forest as the next best. Logistic Regression can be used as a baseline but is not strong enough to be the recommended same-domain IoMT detector with the current feature configuration. In the same-domain, the confusion matrix for the best-performing ML model (XGBoost) is shown in Figure 6, confirming strong discrimination between benign and attack traffic.

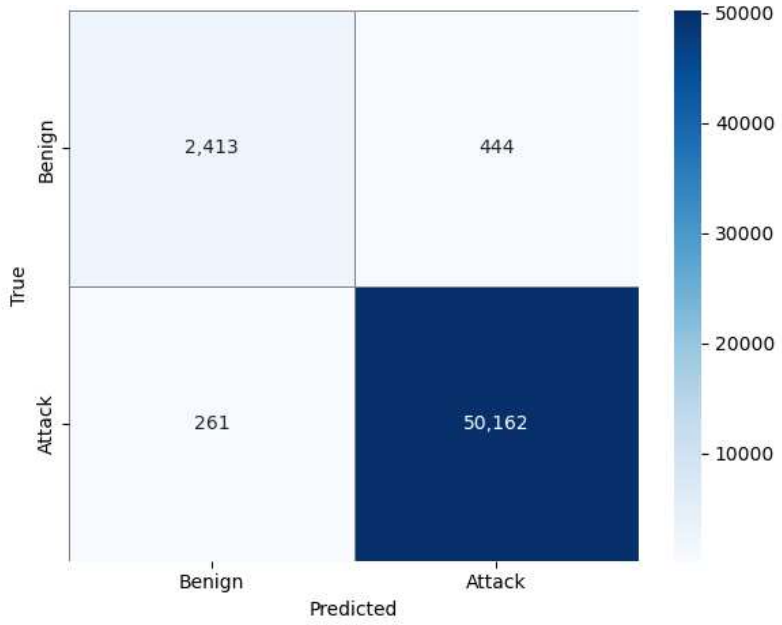


Fig. 6 Confusion Matrix: IoMT to IoMT (XGBoost)

4.3 Same-domain Performance on CICIoT2023 Dataset

The second experiment of the same-domain was carried out in the IoT-to-IoT scenario using the CICIoT2023 dataset. The sampled IoT data in this experiment contained 311,268 instances, with a distribution of 211,268 attack and 100,000 benign instances. A total of 25 features were selected for this experiment, as shown in Table 11.

Table 11 IoT to IoT performance

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC	Training Time(s)
Logistic Regression	0.9662	0.9979	0.9522	0.9745	0.9903	2.96
Random Forest	0.9796	0.9930	0.9768	0.9848	0.9974	72.99
XGBoost	0.9807	0.9940	0.9774	0.9856	0.9976	5.09

On the CICIoT2023 dataset, as with the IoMT benchmark, XGBoost achieved the best overall same-domain performance. Random Forest was still very competitive, followed by Logistic Regression with slightly lower performance.

This consistency between the two same-domain benchmarks indicates that XGBoost is a good choice when the training and test distributions are similar. But it was less efficient. Random Forest took 72.99 seconds to train, while XGBoost took 5.09 seconds and Logistic Regression took 2.96 seconds. Therefore, even though Random Forest performed very well in the same-domain settings, XGBoost provided a better trade-off between performance and computational cost. Figure 7 illustrates the same-domain performance of three Models on IoT-to-IoT settings.

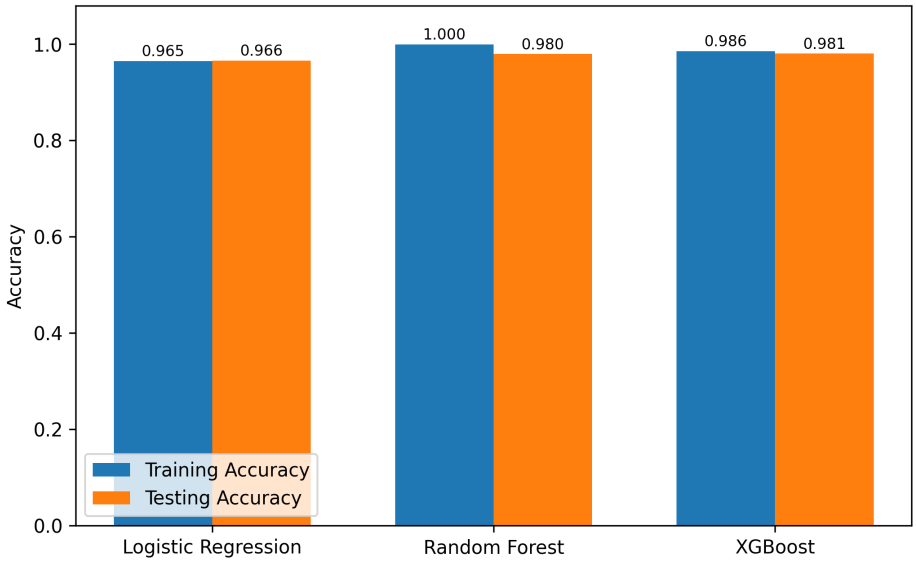


Fig. 7 IoT to IoT: Training vs Testing Accuracy

The confusion matrix in the same-domain (IoT to IoT) for the best-performing ML model (XGBoost) is shown in Figure 8, confirming robust identification of both attack and benign traffic.

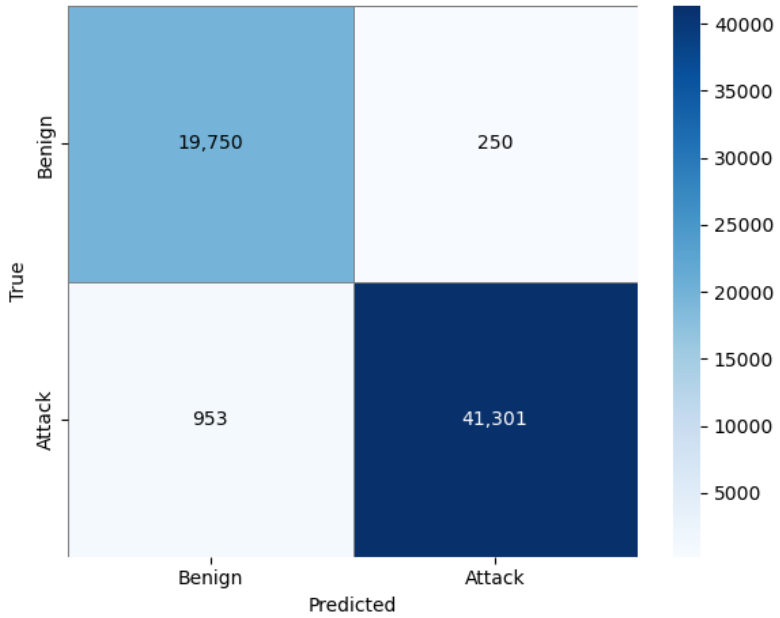


Fig. 8 Confusion Matrix: IoT to IoT (XGBoost)

4.4 Cross-domain Transfer from CICIoMT2024 to CICIoT2023 Dataset

The IoMT-to-IoT experiment was the primary cross-dataset experiment. In this case, model training was based on the CICIoMT2024 dataset and testing on the CICIoT2023 dataset. This experiment was crucial from a methodological perspective as it verifies the ability of models trained for IoMT data to be applied to a more general IoT environment. The IoMT source matrices had 94,490 training instances, 23,623 validation instances, and 15 selected features after feature selection and crash-safe preprocessing, and the performance from IoMT to IoT is shown in Table 12.

In Table 13, the cross-domain performance from IoMT to IoT was very different from the same-domain performance. Logistic Regression performed best in the transfer learning, with 89.65% accuracy, 90.86% F1-score, and 0.9490 ROC-AUC. On the other hand, Random Forest and XGBoost both had high attack biases and predicted most target-domain traffic as malicious. While XGBoost still achieved

Table 12 Cross-domain IoMT to IoT Performance

Model	External Accuracy	External Precision	External Recall	External F1-score	External ROC-AUC	Validation F1
Logistic Regression	0.8965	0.9683	0.8558	0.9086	0.9490	0.9636
Random Forest	0.6008	0.6008	1.0000	0.7506	0.2821	0.9969
XGBoost	0.6008	0.6008	1.0000	0.7506	0.9851	0.9983

a high external ROC-AUC of 0.9851, its threshold-based classification failed to detect benign traffic, which shows that the higher the probability-ranking performance, the better the decision-making performance does not guarantee useful decision performance in transfer learning.

Table 13 Class-wise cross-domain results of IoMT to IoT

Model	Benign Precision	Benign Recall	Benign F1	Attack Precision	Attack Recall	Attack F1
Logistic Regression	0.8153	0.9578	0.8808	0.9683	0.8558	0.9086
Random Forest	0.0000	0.0000	0.0000	0.6008	1.0000	0.7506
XGBoost	1.0000	0.0000	0.0000	0.6008	1.0000	0.7506

Figure 9 illustrates the change in model performance when CICIoMT2024 training was performed and CICIoT2023 testing was performed, and it clearly indicates that LR managed strong cross-domain accuracy, but the ensemble models showed significant performance decline.

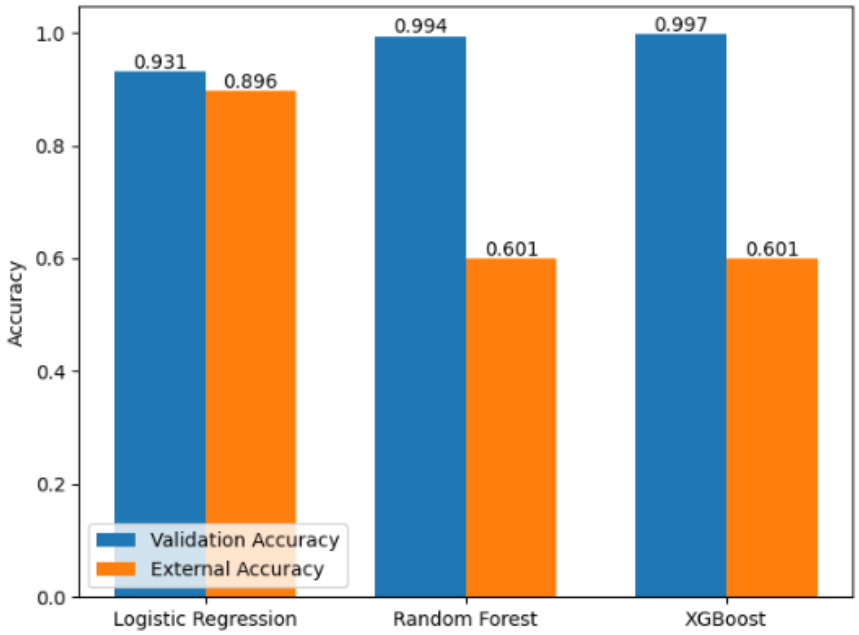


Fig. 9 IoMT to IoT: Validation vs External Accuracy

The confusion matrix in Figure 10 demonstrates the predictive behavior of the most balanced model when transferring from CICIoMT2024 to CICIoT2023 and indicates much-improved preservation of the benign class compared with the nonlinear ensemble models.

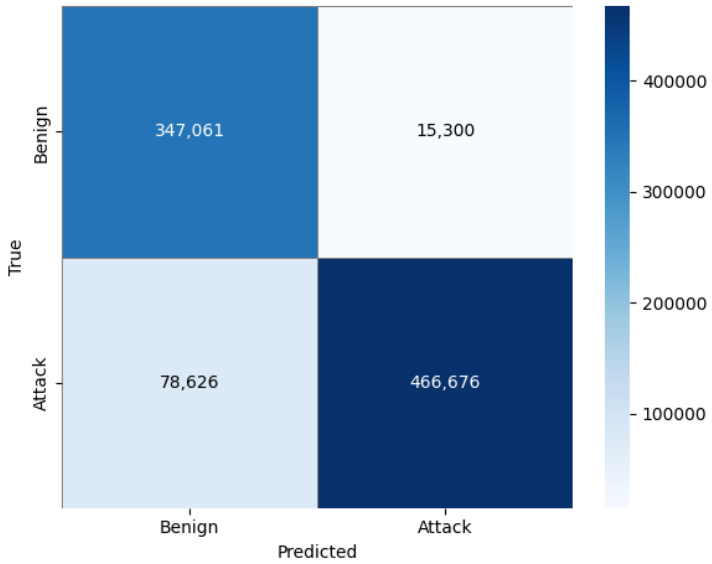


Fig. 10 Confusion Matrix: IoMT to IoT (Logistic Regression)

4.5 Cross-domain Transfer from CICIoT2023 to CICIoMT2024 Dataset

The IoT to IoMT experiment was carried out to verify whether the same directional bias exists when the source and target datasets are swapped. In this experiment, models were trained on the CICIoT2023 dataset and tested on the CICIoMT2024 dataset. The IoMT dataset contained 1,614,182 instances (37,607 benign and 1,576,575 attack). The cross-domain performance from IoT to IoMT is shown in Table 14.

Table 14 IoT to IoMT performance

Model	External Accuracy	External Precision	External Recall	External F1-score	External ROC-AUC	Validation F1
Logistic Regression	0.9786	0.9881	0.9900	0.9891	0.7469	0.9749
Random Forest	0.5003	0.9557	0.5121	0.6669	0.0642	0.9841
XGBoost	0.9754	0.9804	0.9947	0.9875	0.2946	0.9848

At the aggregate level, Logistic Regression and XGBoost had similarly high external F1-scores. However, again, class-specific evaluation shows a key difference: Logistic Regression maintained much better benign-class performance than XGBoost, and Random Forest completely collapsed. Logistic Regression's benign F1-score was 0.5212, while XGBoost achieved 0.2387, and Random Forest 0.0005, as shown in Table 15.

Table 15 Class-wise results of IoT to IoMT

Model	Benign Precision	Benign Recall	Benign F1	Attack Precision	Attack Recall	Attack F1
Logistic Regression	0.5443	0.4999	0.5212	0.9881	0.9900	0.9891
Random Forest	0.0003	0.0059	0.0005	0.9557	0.5121	0.6669
XGBoost	0.4285	0.1654	0.2387	0.9804	0.9947	0.9875

This finding in Table 15 demonstrates that the weakness was not specific to the IoMT-to-IoT transfer. Again, the stronger same-domain ensemble models are less reliable in responding to benign classes, while Logistic Regression maintains a better class balance. Thus, the cross-domain performance degradation observed in this study was symmetric for the two directions of transfer, with varying degrees and patterns across models.

Figure 11 illustrates the change in model performance when CICIoT2023 training was performed and CICIoMT2024 testing was performed, and it clearly indicates that LR and XGBoost achieved high accuracy, but RF did not perform well on cross-domain transfer

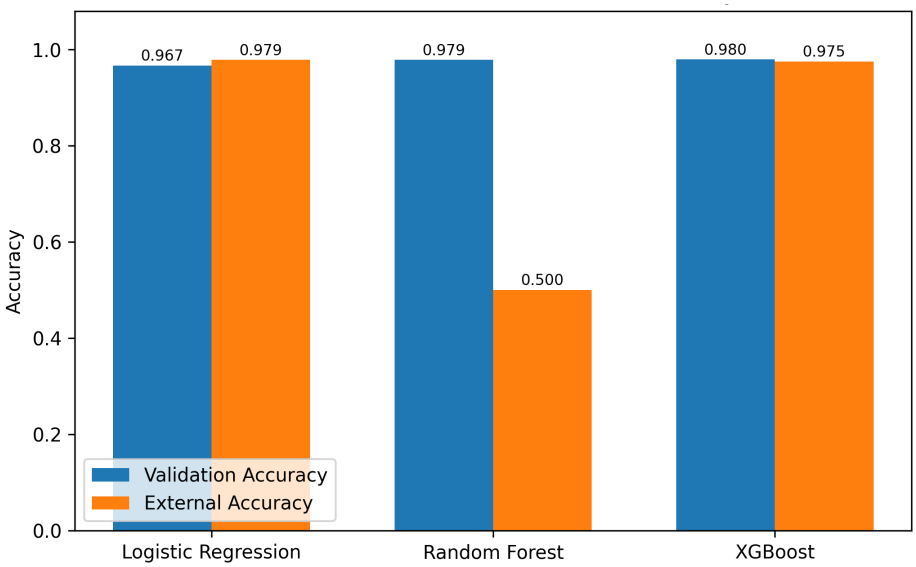


Fig. 11 IoMT to IoT: Validation vs External Accuracy

The confusion matrix in Figure 12 demonstrates that Logistic Regression presented the most balanced reverse transfer, particularly in the recognition of benign classes, compared to the other models.

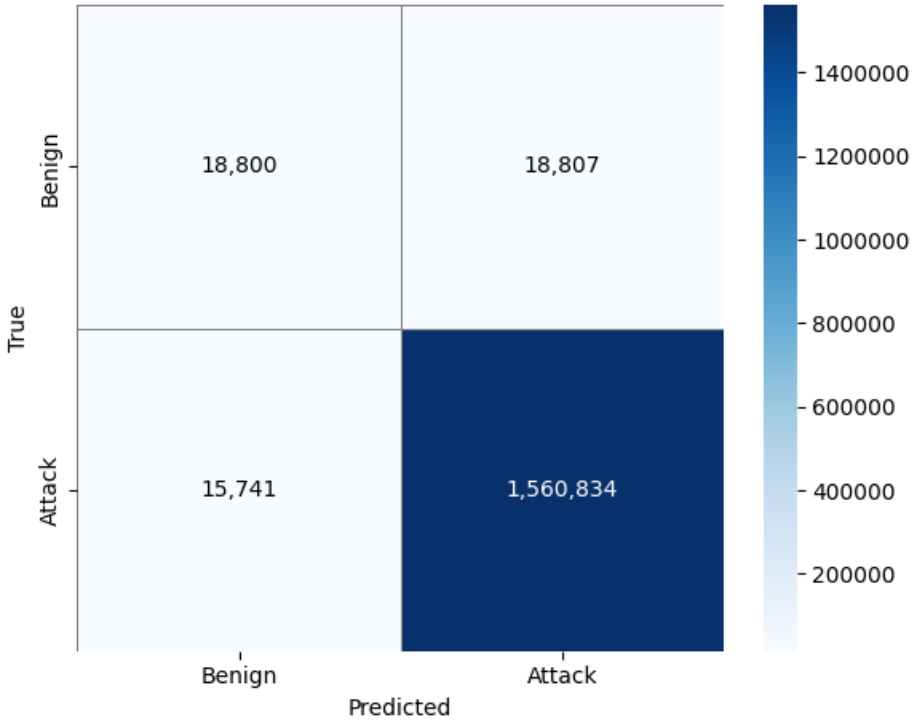


Fig. 12 Confusion Matrix: IoT to IoMT (Logistic Regression)

4.6 Summary of Same and Cross-Domain best performing ML models

The overall results in Table 16 show a clear pattern that in the same-domain experiments, XGBoost performed best for both CICIoMT2024 and CICIoT2023 datasets. In cross-domain experiments, Logistic Regression was the most consistent for benign traffic. Random Forest performed well in the same-domain experiments, but was the least robust in cross-domain experiments. The result of model ranking inversion is a major contribution of the paper: if evaluation is limited to same-domain benchmarks, XGBoost would have appeared as the best model for all tasks. But when we consider transfer learning, the linear model is more robust and balanced.

Table 16 Best performing models summary

Experimental Setting	Best-Performing Model	Main Observation
IoMT IoMT	XGBoost	Highest in-domain IoMT performance
IoT IoT	XGBoost	Highest in-domain IoT performance
IoMT IoT	Logistic Regression	Most balanced transfer to IoT
IoT IoMT	Logistic Regression	Strongest benign-class transfer back to IoMT

Figure 13 illustrates the F1 score comparison of ML models across all four experimental scenarios.

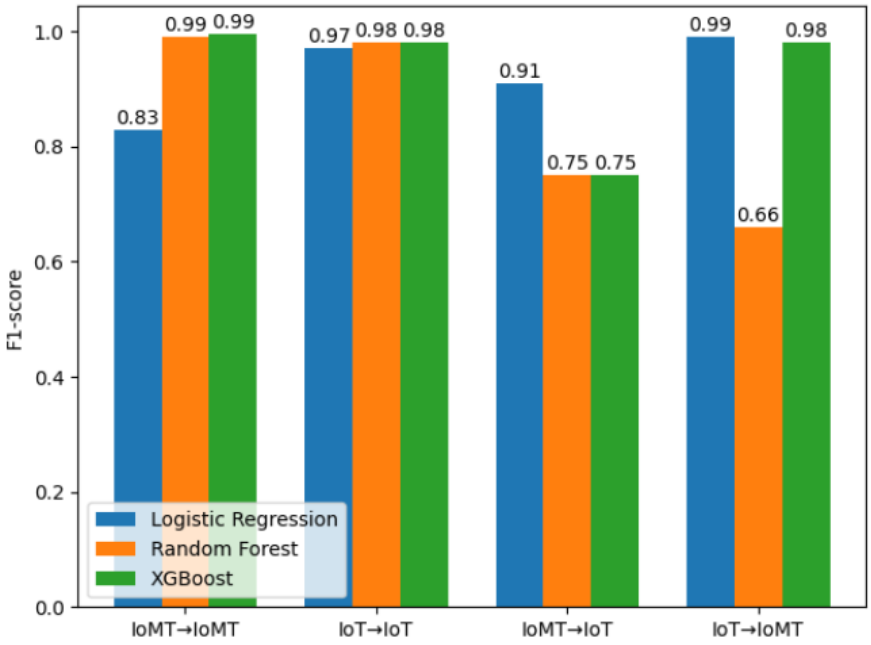


Fig. 13 Overall F1 score comparison across all Models

Figure 14 illustrates the overall accuracy performance of ML models across all four experimental scenarios, and it demonstrates that in the same-domain experiments XGBoost dominated, while in cross-domain experiments LR showed stronger stability.

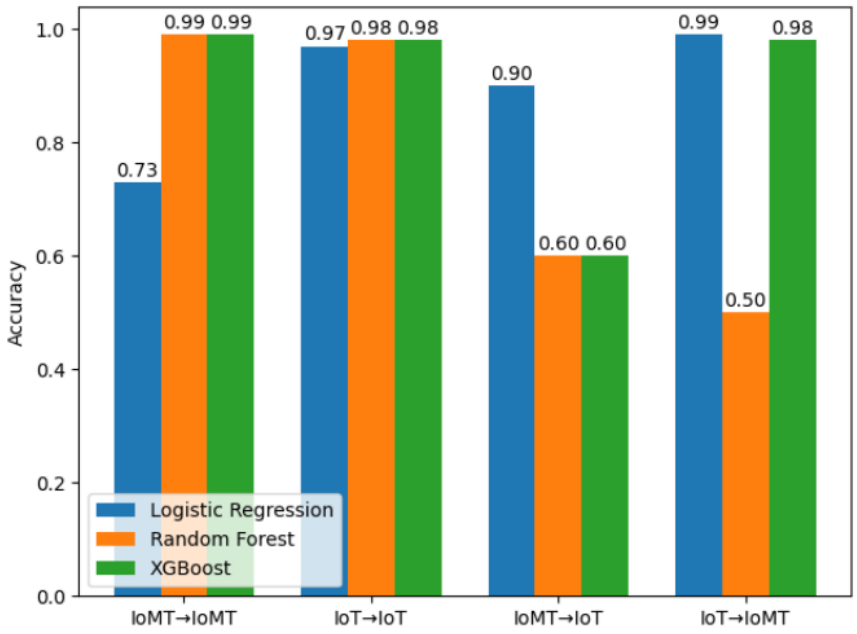


Fig. 14 Overall Accuracy comparison across all Models

4.7 Cross-domain XGBoost Threshold Analysis

The cross-domain using the XGBoost framework in Table 17 was tuned to determine whether the difference in performance was the result of decision threshold selection. This was done in both the IoMT to IoT and IoT to IoMT directions.

Table 17 Cross-domain XGBoost threshold analysis results

Transfer Direction	**Best Threshold by Macro-F1**	**Main Outcome**
IoMT IoT	0.99	Benign recovery remained negligible
IoT IoMT	0.50	Threshold changes gave only marginal class-balance benefit

For IoMT to IoT, adjusting the threshold did not improve benign recognition. The best threshold provided benign recall of only 0.0012, with benign F1 still very low. For IoT to IoMT, the effect of threshold tuning slightly shifted the balance, with best macro-F1 near the default threshold, and only minimal improvement in best balanced accuracy.

The figure 15 demonstrates the impact of threshold adjustment on overall classification accuracy, and that changing the threshold does not overcome the transfer-performance challenges

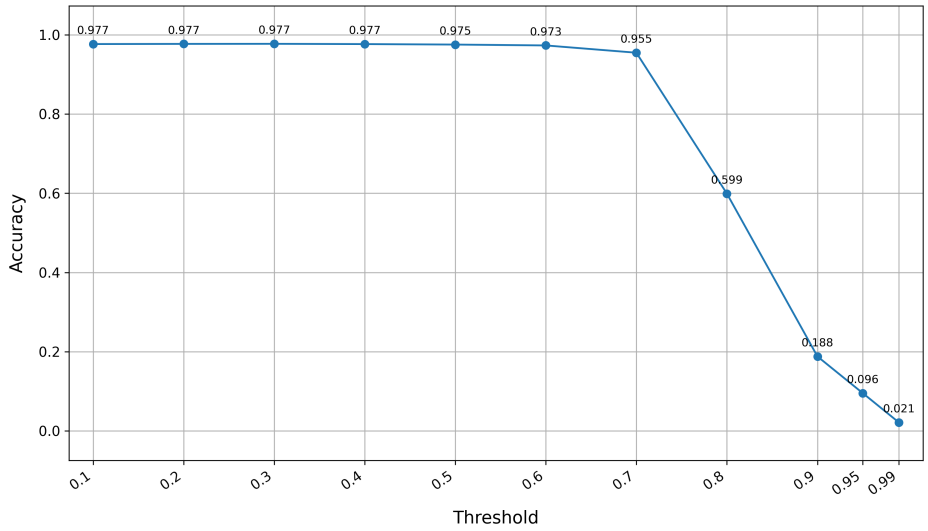


Fig. 15 Variation of accuracy across decision thresholds for XGBoost in IoT to IoMT transfer experiment.

Figure 16 shows the effect of threshold adjustment on the macro-F1 score and suggests that only minor class balance improvement was provided.

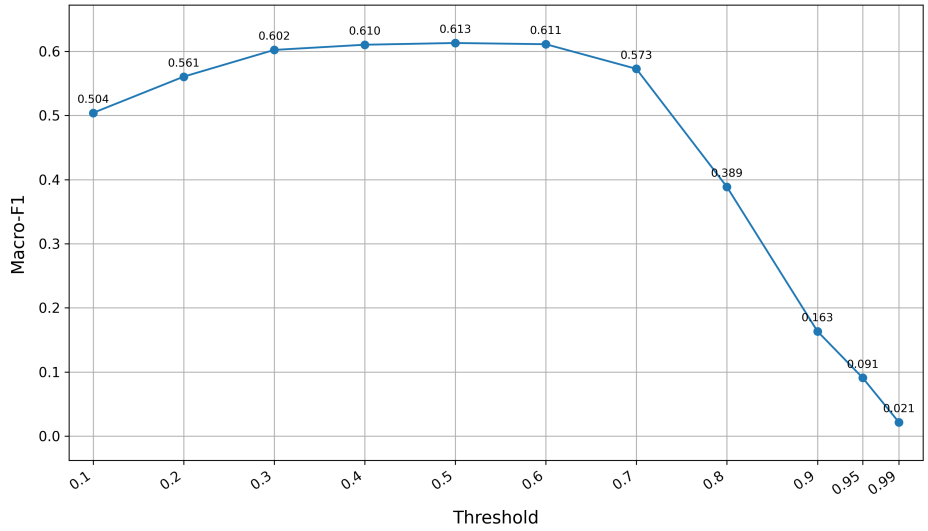


Fig. 16 Variation of Macro F1 across decision thresholds for XGBoost in IoT to IoMT transfer experiment.

This figure 17 shows the impact of threshold adjustment on balanced accuracy, and confirms that only limited class balance performance was achieved.

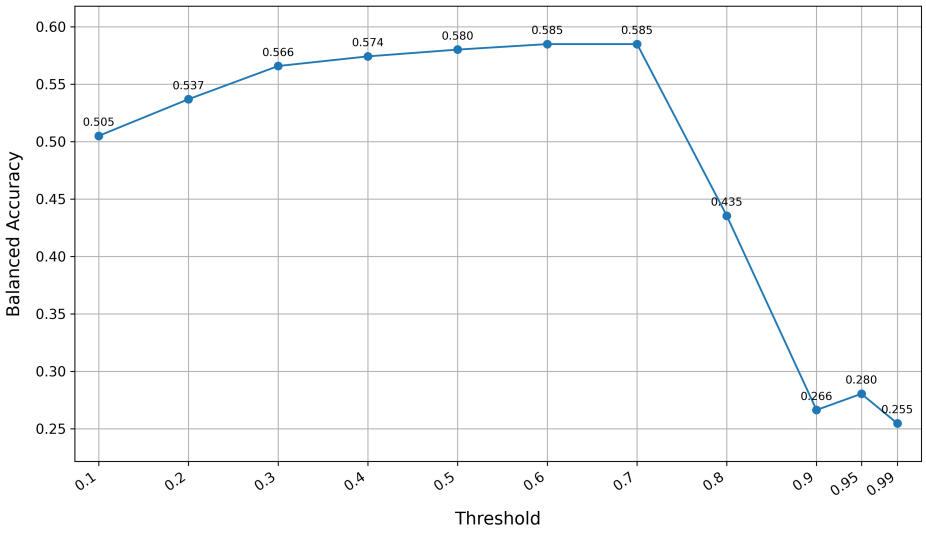


Fig. 17 Variation of balanced accuracy across decision thresholds for XGBoost in the IoT to IoMT transfer experiment.

These results suggest that the major failure in transfer is not simply due to a default threshold setting. Rather, the findings indicate domain shift is the primary cause of failure.

4.8 Compatibility Assessment of Edge-IIoTset

The Edge-IIoTset was considered an external robustness dataset. To examine the possibility of direct transfer evaluation, a schema inspection was conducted between CICIoMT2024 and some Edge-IIoTset files. This involved both raw and normalized feature names, and the cardinalities at both levels were zero. CICIoMT2024 included flow-statistical descriptors such as *header_length*, *protocol_type*, *rate*, *iat*, *covariance*, and *variance*. In contrast, Edge-IIoTset contained packet- and protocol-based attributes including *frame_time*, *ip_src_host*, *tcp_dstport*, *dns_qry_name*, *mqtt_topic*, and *attack_type*. Since in Table 18 there was no overlap in the feature space, direct transfer would have been methodologically invalid.

Table 18 Compatibility analysis of feature between CICIoMT2024 and Edge-IIoTset

Criterion	Result
Raw feature overlap	0
Normalized feature overlap	0
Direct IoMT Edge transfer possible	No
Required for future use	Schema harmonization or custom shared feature extraction

The findings in Table 18 are not weaknesses of the study, but enhance the validity by showing that the external robustness was evaluated and no invalid comparisons were made.

5 Conclusion & Future Directions

This study provided an IoMT-centered intrusion detection system, benchmarked on the CICIoMT2024 dataset and cross-evaluated on the CICIoT2023 dataset. Three Machine Learning models, including Random Forest, XGBoost, and Logistic Regression, were trained and evaluated on both same and cross-domain environments. XGBoost achieved the best performance on same-domain data (accuracy 98.68% and F1-score 0.993 on the CICIoMT2024 dataset), suggesting it is the most effective domain classifier. Random Forest also performed well and achieved 98.07% accuracy in the same domain, but Logistic Regression had much lower performance (72.53%) in the same domain.

However, the results of the cross-domain evaluations using CICIoT2023 were different. Logistic Regression showed the most consistent domain transfer performance with 89.65% external accuracy and balanced class representation, while Random Forest and XGBoost performed poorly under domain shift, in some instances failing to achieve 60.08% accuracy with severe class imbalance; also, the

threshold tuning could not resolve this degradation, highlighting that domain shift, especially in benign traffic representation, is the main issue rather than probability misalignment.

Moreover, to evaluate robustness, Edge-IIOTset was also tested as an additional dataset, but because its features were not fully compatible with the CICIoMT2024 dataset, it was not fully integrated into the environment. In summary, the results show that based on the same-domain accuracy, it is not enough to choose the best model for IoMT intrusion detection. Rather, cross-domain performance, benign-class accuracy, and dataset compatibility should be taken into account to develop effective and deployable intrusion detection solutions for real-world IoMT systems.

Future work may explore enhancing cross-domain performance through domain adaptation and feature alignment approaches to address dataset mismatches. Ensemble and linear models may also be combined to improve environmental robustness. In addition, deep learning and AI techniques can be investigated to improve detection accuracy and interpretability. Furthermore, real-time and edge deployment should be explored to determine the practicality of intrusion detection systems in IoMT environments.

Declarations

Clinical trial number

Not applicable.

Funding Statement

The authors gratefully acknowledge Multimedia University for the financial support provided for this work.

Ethics approval and consent to participate

Not applicable.

Consent to publish

Not applicable.

Data Availability Statement

The datasets analysed during the current study are publicly available from third-party repositories. The CICIoMT2024 dataset is available from the Canadian Institute for Cybersecurity (CIC) repository at https://www.unb.ca/cic/datasets/iomt-dataset-2024.html. The CICIoT2023 dataset is available from the Canadian Institute for Cybersecurity (CIC) repository at https://www.unb.ca/cic/datasets/iotdataset-2023.html. The Edge-IIoTset dataset is available from IEEE DataPort at https://doi.org/10.21227/mbc1-1h68.

Competing interests

The authors declare no competing interests.

References

[1] Osman, R.A.: Optimizing iot communication for enhanced data transmission in smart farming ecosystems. Expert Systems with Applications **265**, 125879 (2025)

[2] Alturif, G., Saleh, W., El-Bary, A.A., Osman, R.A.: Towards efficient iot communication for smart agriculture: A deep learning framework. Plos one **19**(11), 0311601 (2024)

[3] 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 (2020). IEEE

[4] Al-Dhief, F.T., Latiff, N.M.A., Malik, N.N.N.A., Salim, N.S., Baki, M.M., Albadr, M.A.A., Mohammed, M.A.: A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms. IEEE Access **8**, 64514–64533 (2020)

[5] Reegu, F.A., Abas, H., Jabbari, A., Akmam, R., Uddin, M., Wu, C.-M., Chen, C.-L., Khalaf, O.I.: [retracted] interoperability requirements for blockchain-enabled electronic health records in healthcare: A systematic review and open research challenges. Security and Communication Networks **2022**(1), 9227343 (2022)

[6] Qadri, Y.A., Nauman, A., Zikria, Y.B., Vasilakos, A.V., Kim, S.W.: The future of healthcare internet of things: a survey of emerging technologies. IEEE Communications Surveys & Tutorials **22**(2), 1121–1167 (2020)

[7] Alshehri, F., Muhammad, G.: A comprehensive survey of the internet of things (iot) and ai-based smart healthcare. IEEE access **9**, 3660–3678 (2020)

[8] Subahi, A.F.: Edge-based iot medical record system: requirements, recommendations and conceptual design. IEEE Access **7**, 94150–94159 (2019)

[9] Dhanvijay, M.M., Patil, S.C.: Internet of things: A survey of enabling technologies in healthcare and its applications. Computer networks **153**, 113–131 (2019)

[10] Dias, D., Paulo Silva Cunha, J.: Wearable health devices—vital sign monitoring, systems and technologies. Sensors **18**(8), 2414 (2018)

[11] Irkham, I., Ibrahim, A.U., Nwekwo, C.W., Al-Turjman, F., Hartati, Y.W.: Current technologies for detection of covid-19: Biosensors, artificial intelligence and internet of medical things (iomt). Sensors **23**(1), 426 (2022)

[12] Chakraborty, T., Roy, P., Nesa, N.: Iomt-based biochip-integrated point-of-care testing for smart healthcare. IEEE internet of things journal **10**(24), 22740–22747 (2023)

[13] Manickam, P., Mariappan, S.A., Murugesan, S.M., Hansda, S., Kaushik, A., Shinde, R., Thipperudraswamy, S.: Artificial intelligence (ai) and internet of medical things (iomt) assisted biomedical systems for intelligent healthcare. Biosensors **12**(8), 562 (2022)

[14] Yang, T., Gentile, M., Shen, C.-F., Cheng, C.-M.: Combining point-of-care diagnostics and internet of medical things (IoMT) to combat the COVID-19 pandemic. MDPI (2020)

[15] Ahmed, S.F., Sharmin, S., Kuldeep, S.A., Lameesa, A., Alam, M.S.B., Liu, G., Gandomi, A.H.: Transformative impacts of the internet of medical things on modern healthcare. Results in Engineering **25**, 103787 (2025)

[16] Stoumpos, A.I., Kitsios, F., Talias, M.A.: Digital transformation in healthcare: technology acceptance and its applications. International journal of environmental research and public health **20**(4), 3407 (2023)

[17] Mabina, A., Rafifing, N., Seropola, B., Monageng, T., Majoo, P.: Challenges in iomt adoption in healthcare: focus on ethics, security, and privacy. Journal of Information Systems and Informatics **6**(4), 3162–3184 (2024)

[18] Al-Abadi, A.A.J., Mohamed, M.B., Fakhfakh, A.: Enhanced random forest classifier with k-means clustering (erf-kmc) for detecting and preventing distributed-denial-of-service and man-in-the-middle attacks in internet-of-medical-things networks. Computers **12**(12), 262 (2023)

[19] Theocharidou, M., Lella, I.: Enisa threat landscape: Health sector. Epub ahead of print (2023)

[20] Mattioli, R., Malatras, A., et al.: Foresight cybersecurity threats for 2030–update. ENISA. Prieiga per internetą:< https://www. enisa. europa. eu/publications/foresight-cybersecuritythreats-for-2030-update-2024-extended-report (2024)

[21] CrowdStrike: Global Threat Report 2025. https://www.crowdstrike.com/en-us/global-threat-report/. Accessed: 2026-04-29 (2025)

[22] Iwendi, C., Anajemba, J.H., Biamba, C., Ngabo, D.: Security of things intrusion detection system

for smart healthcare. Electronics **10**(12), 1375 (2021)

[23] Heidari, A., Jabraeil Jamali, M.A.: Internet of things intrusion detection systems: a comprehensive review and future directions. Cluster Computing **26**(6), 3753–3780 (2023)

[24] Khan, A.A., Faheem, M., Bashir, R.N., Wechtaisong, C., Abbas, M.Z.: Internet of things (iot) assisted context aware fertilizer recommendation. IEEE Access **10**, 129505–129519 (2022)

[25] Khan, A.A., Driss, M., Boulila, W., Sampedro, G.A., Abbas, S., Wechtaisong, C.: Privacy preserved and decentralized smartphone recommendation system. IEEE Transactions on Consumer Electronics **70**(1), 4617–4624 (2023)

[26] David, J., Thomas, C.: Discriminating flash crowds from ddos attacks using efficient thresholding algorithm. Journal of Parallel and Distributed Computing **152**, 79–87 (2021)

[27] Zheng, J., Li, Q., Gu, G., Cao, J., Yau, D.K., Wu, J.: Realtime ddos defense using cots sdn switches via adaptive correlation analysis. IEEE Transactions on Information Forensics and Security **13**(7), 1838–1853 (2018)

[28] Sarker, I.H.: Machine learning: Algorithms, real-world applications and research directions. SN computer science **2**(3), 1–21 (2021)

[29] Doménech, J., Martin-Faus, I.V., Mhiri, S., Pegueroles, J.: Ensuring patient safety in iomt: A systematic literature review of behavior-based intrusion detection systems. Internet of Things **28**, 101420 (2024)

[30] Weber, S.B., Stein, S., Pilgermann, M., Schrader, T.: Attack detection for medical cyber-physical systems–a systematic literature review. IEEE Access **11**, 41796–41815 (2023)

[31] Nagarajan, G., Margala, M., Chakrabarti, P., Minu, R., *et al.*: A trust-centric approach to intrusion detection in edge networks for medical internet of thing ecosystems. Computers and Electrical Engineering **115**, 109129 (2024)

[32] Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J.C., Rodriguez, J.: An anomaly-based intrusion detection system for internet of medical things networks. Electronics **10**(21), 2562 (2021)

[33] RM, S.P., Maddikunta, P.K.R., Koppu, S., Gadekallu, T.R., Chowdhary, C.L., Alazab, M., *et al.*: An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture. Computer Communications **160**, 139–149 (2020)

[34] Kumar, P., Gupta, G.P., Tripathi, R.: An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks. Computer Communications **166**, 110–124 (2021)

[35] Huda, S., Islam, M.R., Abawajy, J., Kottala, V.N.V., Ahmad, S.: A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors **24**(16), 5282 (2024)

[36] 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)

[37] Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Ahmad Khan, R.: Healthcare data breaches: insights and implications. In: Healthcare, vol. 8, p. 133 (2020). MDPI

[38] Hernandez-Jaimes, M.L., Martinez-Cruz, A., Ramírez-Gutiérrez, K.A., Feregrino-Uribe, C.: Artificial intelligence for iomt security: A review of intrusion detection systems, attacks, datasets and cloud–fog–edge architectures. Internet of Things **23**, 100887 (2023)

[39] Rasool, R.U., Ahmad, H.F., Rafique, W., Qayyum, A., Qadir, J.: Security and privacy of internet

of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ml. Journal of Network and Computer Applications **201**, 103332 (2022)

[40] Weber, S.B., Stein, S., Pilgermann, M., Schrader, T.: Attack detection for medical cyber-physical systems–a systematic literature review. IEEE Access **11**, 41796–41815 (2023)

[41] Zikria, Y.B., Afzal, M.K., Kim, S.W.: Internet of multimedia things (iomt): Opportunities, challenges and solutions. Sensors **20**(8), 2334 (2020)

[42] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., Atkinson, R.: Shallow and deep networks intrusion detection system: A taxonomy and survey. arXiv preprint arXiv:1701.02145 (2017)

[43] Liu, H., Lang, B.: Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences **9**(20), 4396 (2019)

[44] Rasool, R.U., Ahmad, H.F., Rafique, W., Qayyum, A., Qadir, J.: Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ml. Journal of Network and Computer Applications **201**, 103332 (2022)

[45] Thakkar, A., Lohiya, R.: A review of the advancement in intrusion detection datasets. Procedia Computer Science **167**, 636–645 (2020)

[46] Anis, F.M., AlAbdullatif, M., Aljbli, S., Hammoudeh, M.: A survey on the applications of deep learning in network intrusion detection systems to enhance network security. IEEE Access (2025)

[47] Aldweesh, A., Derhab, A., Emam, A.Z.: Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems **189**, 105124 (2020)

[48] Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M., Ahmad, R.: Machine learning and deep learning approaches for cybersecurity: A review. IEEE Access **10**, 19572–19585 (2022)

[49] Mukhaini, G.A., Anbar, M., Manickam, S., Al-Amiedy, T.A., Al Momani, A.: A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in internet of things networks. Journal of King Saud University-Computer and Information Sciences **36**(1), 101866 (2024)

[50] Shanmugam, V., Razavi-Far, R., Hallaji, E.: Addressing class imbalance in intrusion detection: A comprehensive evaluation of machine learning approaches. Electronics **14**(1), 69 (2024)

[51] 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). Transactions on Emerging Telecommunications Technologies **33**(6), 4049 (2022)

[52] Weber, S.B., Stein, S., Pilgermann, M., Schrader, T.: Attack detection for medical cyber-physical systems–a systematic literature review. IEEE Access **11**, 41796–41815 (2023)

[53] Doménech, J., León, O., Siddiqui, M.S., Pegueroles, J.: Evaluating and enhancing intrusion detection systems in iomt: The importance of domain-specific datasets. Internet of Things **32**, 101631 (2025)

[54] Jaiswal, R., Andersen, P.-A., Cenkeramaddi, L.R., Jiao, L., Granmo, O.-C.: A tsetlin machine-driven intrusion detection system for next-generation iomt security. arXiv preprint arXiv:2604.03205 (2026)

[55] Albarrak, A.M.: An adaptive intrusion detection system for securing the internet of medical things using deep learning. EAI Endorsed Transactions on Internet of Things **11** (2024)

[56] Mohammad, A.E., Abdulrahman, A.A.: An intrusion detection for internet of medical things based on deep learning techniques. Ibn AL-Haitham Journal For Pure and Applied Sciences

39(1), 317–332 (2026)

[57] Berguiga, A., Harchay, A., Massaoudi, A.: Hids-iomt: A deep learning-based intelligent intrusion detection system for the internet of medical things. IEEE Access (2025)

[58] Hafid, A., Rahouti, M., Aledhari, M.: Optimizing intrusion detection in iomt networks through interpretable and cost-aware machine learning. Mathematics **13**(10), 1574 (2025)

[59] Zachos, G., Mantas, G., Porfyrakis, K., Rodriguez, J.: Implementing anomaly-based intrusion detection for resource-constrained devices in iomt networks. Sensors **25**(4), 1216 (2025)

[60] Cybersecurity, C.I.: CICIoMT2024 Dataset. https://www.unb.ca/cic/datasets/iomt-dataset-2024.html (2024)

[61] Cybersecurity, C.I.: CICIoT2023 Dataset. https://www.unb.ca/cic/datasets/iotdataset-2023.html (2023)

[62] Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L., Janicke, H.: Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications. IEEE DataPort (2022). https://doi.org/10.21227/mbc1-1h68

[63] Kundu, S., Patkar, S.S., Mishra, S.M., Trivedi, G., Merchant, F.: A 360-degree review of tsetlin machines: Concepts, applications, analysis, and the future. Authorea Preprints

[64] Granmo, O.-C.: The tsetlin machine–a game theoretic bandit driven approach to optimal pattern recognition with propositional logic. arXiv preprint arXiv:1804.01508 (2018)

[65] Mitchell, R., Chen, R.: Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. IEEE Transactions on Dependable and Secure Computing **12**(1), 16–30 (2014)

[66] Nawaal, B., Haider, U., Khan, I.U., Fayaz, M.: Signature-based intrusion detection system for iot. In: Cyber Security for Next-generation Computing Technologies, pp. 141–158. CRC Press, ??? (2024)