AIMS Mathematics, 10(11): 25274–25306.
DOI:10.3934/math.20251119
Received: 10 August 2025
Revised: 04 October 2025
Accepted: 13 October 2025
Published: 04 November 2025

https://www.aimspress.com/journal/Math

Research article

Securing healthcare systems and optimizing data analytics through IoMT threat detection

Abdulmajeed Atiah Alharbi[1], **Maher Alharby**[2] **and Ahmad Ali Hanandeh**[3,*]

[1] Department of Mathematics, College of Science, Taibah University, Madinah, Saudi Arabia
[2] Department of Cybersecurity, College of Computer Science and Engineering, Taibah University, Madinah, 42353, Saudi Arabia
[3] Department of Mathematics, Faculty of Science, Islamic University of Madinah, Madinah, 42351, Saudi Arabia

* **Correspondence:** Email: hanandeh@iu.edu.sa; Tel: +962-791-542-383.

Abstract: The integration of Internet of Medical Things (IoMT) devices into are systems has raised significant cybersecurity concerns, especially regarding threats to patient safety and the protection of sensitive medical data. This research proposes a novel hybrid machine learning framework aimed at improving the detection and mitigation of cyberattacks in IoMT environments. Our approach combines random forest, AdaBoost, and bagging algorithms to identify various attack vectors across different IoMT networks. We evaluate our framework using a comprehensive IoMT traffic dataset that includes different communication protocols. Using advanced statistical profiling and ensemble classification models, our system achieves high detection performance while significantly reducing false positive rates compared to traditional methods. The hybrid model demonstrates an exceptional precision of 99.92%, ensuring reliable differentiation between benign and malicious network traffic and minimizing disruptions in critical healthcare environments. Experimental validation across various attack scenarios confirms the effectiveness of the framework in addressing the unique security challenges posed by resource-constrained IoMT devices and heterogeneous communication protocols.

Keywords: internet of medical things (IoMT); cybersecurity; cyberattack detection; machine learning (ML); hybrid model; CICIoMT2024 dataset
Mathematics Subject Classification: 62H30, 68T05

1. Introduction

The Internet of Medical Things (IoMT) is enhancing modern healthcare by facilitating the integration of interconnected smart medical devices for real-time patient monitoring, automated

treatment delivery, and remote diagnostics. This technological advancement is reshaping healthcare infrastructure and supporting national digital transformation initiatives, such as Saudi Arabia's Vision 2030. The IoMT encompasses a diverse array of medical devices, including wearable sensors, implantable devices, advanced diagnostic tools, and hospital management systems. These devices communicate through various protocols, including Wi-Fi, Bluetooth Low Energy (BLE), and Message Queuing Telemetry Transport (MQTT).

While this connectivity enhances clinical capabilities and patient outcomes, it also presents significant cybersecurity challenges that threaten the confidentiality, integrity, and availability of sensitive medical data and critical healthcare operations. Recent industry analyses indicate a concerning 15% annual increase in critical IoMT vulnerabilities [41]. These vulnerabilities expose healthcare systems to sophisticated cyber threats, including reconnaissance attacks, device spoofing, denial-of-service (DoS) attacks, and advanced persistent threats (APTs).

The unique characteristics of IoMT environments further complicate these security challenges. Medical devices often have limited computational resources, proprietary firmware, legacy systems, and a mix of diverse technology stacks. The critical nature of healthcare operations, where system downtime can threaten patient safety, creates a complex security landscape that traditional cybersecurity measures often fail to address effectively. In addition, strict regulatory requirements in healthcare, such as HIPAA compliance and data sovereignty mandates, further complicate security implementations [22].

Machine learning (ML) techniques have emerged as effective solutions to address complex cybersecurity challenges in IoMT environments. Recent research studies demonstrate that ensemble learning frameworks, particularly stacking and voting classifiers, can achieve remarkable real-time multiclass detection accuracies exceeding 99% in IoMT networks [1]. Moreover, interpretable and cost-sensitive ML models show that robust security can ensure both efficiency and transparency in clinical settings [20]. These advancements can effectively handle the changing threats in IoMT environments.

However, the development and validation of ML-based security solutions are hindered by dataset limitations. Many existing IoMT datasets suffer from insufficient scale, limited protocol diversity, unrealistic attack simulations, and inadequate representation of real-world IoMT network behaviors. The introduction of datasets like CICIoMT2024 helps overcome these limitations by offering extensive multi-protocol traffic data and attack coverage, facilitating better evaluation of adaptive learning models that manage class imbalance, concept drift, and heterogeneous feature spaces [14]. Building on these foundations, recent research has investigated various ML approaches for enhancing IoMT security. Federated learning (FL) frameworks have shown potential in creating distributed and privacy-preserving intrusion detection systems (IDS) that uphold data integrity requirements [30]. Ensemble methods, especially random forest (RF) and adaptive boosting (AdaBoost), have consistently exhibited superior performance in both accuracy and scalability within heterogeneous IoMT environments [13]. Furthermore, interpretable ML models have gained attention for their ability to offer operational transparency along with high detection accuracy [20].

Despite these advancements, significant gaps persist in current IoMT security approaches. Existing solutions often lack comprehensive evaluations across different IoMT protocols, overlook the resource limitations of medical devices, and fail to meet real-time performance demands essential for healthcare. Additionally, many proposed frameworks remain theoretical without practical implementation

validation or consideration of deployment challenges in real healthcare environments [29].

To address these limitations, this paper proposes a comprehensive ML-based intrusion detection framework specifically tailored for IoMT environments. Our approach integrates advanced preprocessing techniques and a hybrid ensemble learning architecture that combines RF, AdaBoost, and bootstrap aggregating (bagging) algorithms. The framework is assessed using benchmark IoMT traffic datasets that cover a variety of device types, network protocols, and realistic attack scenarios, ensuring thorough validation across the full spectrum of IoMT security challenges.

The main contributions of this work are threefold:

1) We propose a novel hybrid ensemble learning framework that integrates RF, AdaBoost, and bagging algorithms to enhance the detection of cyberattacks in IoMT environments. This framework leverages the complementary strengths of each algorithm to create a more robust and adaptable intrusion detection system, offering a superior alternative to traditional single-model approaches.
1. 2) We rigorously evaluate our framework using the CICIoMT2024 dataset, a comprehensive multi-protocol resource that accurately reflects the diversity and complexity of IoMT networks. The evaluation demonstrates the model's ability to effectively handle a variety of attack scenarios and communication protocols, confirming its robustness and applicability in real-world IoMT environments.
3) Our hybrid model significantly outperforms existing intrusion detection systems in terms of accuracy, precision, recall, and F1-score. By minimizing false positives, the model ensures reliable detection of cyberattacks while reducing unnecessary operational disruptions, which is particularly crucial in healthcare settings where false alarms can compromise patient safety and operational efficiency.

Our experimental evaluation demonstrates that the proposed hybrid ML framework achieves state-of-the-art performance, with precision rates reaching 99.92% in binary attack detection while maintaining exceptionally low false positive rates. This high precision ensures reliable identification of malicious traffic while minimizing operational disruptions caused by false alarms, which is crucial in healthcare environments where unnecessary alerts can lead to alert fatigue and potentially threaten patient safety.

The remainder of this article is structured as follows. Section 2 provides an in-depth analysis of cybersecurity threats and vulnerabilities specific to IoMT environments. Section 3 reviews related work on IoMT security and ML-based IDS. Section 4 discusses ML models for threat detection. Section 5 elaborates on the proposed methodology, including preprocessing of the dataset, feature engineering, and hybrid ensemble learning architecture. Section 6 presents the experimental setup, performance evaluation, and a comparative analysis with existing approaches. Finally, Section 7 concludes the paper with a discussion of the findings and future research directions.

2. Cybersecurity challenges in internet of medical things

The increase in the number of devices on the IoMT has fundamentally transformed modern healthcare delivery. This transformation enables connectivity between medical equipment, healthcare providers, and patients. However, it has also created a complex ecosystem in which life-critical medical

devices continuously generate, transmit, and process sensitive health data across interconnected networks. As a result, digital transformation has expanded the attack surface, leading to complex cybersecurity challenges that can directly affect patient safety, data privacy, and the continuity of healthcare services.

To understand the cybersecurity of the IoMT, it is essential to examine the various attack vectors that threaten these interconnected medical systems. IoMT environments are diverse, featuring devices with limited resources, different communication protocols, and varying levels of security measures. This diversity creates unique vulnerabilities that differ significantly from traditional IT security issues. These vulnerabilities are particularly alarming because cyberattacks on medical devices can lead to immediate and potentially life-threatening consequences for patients.

IoMT devices operate over various communication protocols, including Wi-Fi, Bluetooth, Zigbee, and MQTT, each of which has distinct security vulnerabilities that serve as a foundation for network-based attacks. DoS and distributed DoS (DDoS) attacks pose critical risks by overwhelming device networks with excessive traffic. This can threaten life-critical devices, such as infusion pumps, ventilators, or cardiac monitors [19, 36]. The impact of such attacks extends beyond service disruption, as they can compromise patient safety and affect clinical decision-making processes. Man-in-the-middle (MITM) attacks enable adversaries to intercept or manipulate sensitive medical data during transmission between devices and healthcare systems. These attacks can lead to compromised important sign readings, altered treatment protocols, or unauthorized access to patient health records [6, 19]. In addition, replay and packet injection attacks enable malicious actors to retransmit captured legitimate packets or introduce falsified data into device communications [6, 37]. The use of unencrypted wireless protocols in many IoMT implementations increases the risk of eavesdropping and traffic analysis attacks, enabling the passive management of sensitive patient data and device communications. [17, 19].

The limited resources and computational power of many IoMT devices create significant security risks. One significant threat is firmware manipulation attacks, in which attackers can modify or replace the firmware of a device. This can change the operation of the device, disrupt medical services, or introduce persistent malware that escapes detection by standard security scans [19, 26, 33]. These attacks are particularly concerning as they can compromise device integrity. Physical tampering is another critical vulnerability, particularly in healthcare environments where medical devices may be deployed in less secure locations or require frequent physical access for maintenance. Attackers in physical proximity to devices may exploit open diagnostic ports, insecure hardware interfaces, or inadequate physical security controls to extract sensitive data, inject malware, or bypass authentication mechanisms [17, 19]. Although less common due to their technical complexity, side-channel attacks can present sophisticated threats by analyzing timing variations to uncover cryptographic keys or sensitive patient information [19].

Application-layer vulnerabilities arise from the complexities of software integrations, inadequate input validation, and the interconnected nature of hospital information systems. Various injection attacks, such as SQL injection, code injection, and XML injection, can exploit deficiencies in input validation within device interfaces or centralized management dashboards. This exploitation may lead to unauthorized database manipulation, unauthorized extraction of electronic health records, or command injection [6, 19]. Web-based interfaces for the IoMT, used by healthcare professionals, are particularly vulnerable to browser-related security issues. These vulnerabilities can

result in credential theft, session hijacking, or unauthorized administrative actions within medical systems [19]. Furthermore, weaknesses in authentication and authorization mechanisms create significant security gaps in many IoMT implementations. The lack of robust password policies, multi-factor authentication, and effective access control measures allows for credential-based attacks, including brute-force attacks and privilege escalation [18, 19].

The evolution of malware, ransomware, and botnet attacks directed at healthcare infrastructure poses an increasing threat to the security of the IoMT. Medical-specific variants of established malware families, such as those derived from the Mirai botnet that target healthcare environments [5, 37]. Ransomware attacks pose particularly severe risks by encrypting or disabling critical medical devices, which can halt patient care operations [36]. Furthermore, attacks aimed at data integrity and privacy, such as manipulating sensor readings, treatment logs, or diagnostic results, can have severe impacts on patient health outcomes. The unauthorized extraction of sensitive medical records not only threatens patient confidentiality, but also infringes regulatory compliance obligations [6, 17, 49].

Emerging technologies such as blockchain, artificial intelligence, and FL in IoMT systems introduce new attack surfaces and distinct security concerns. These advanced architectures can be vulnerable to novel attack vectors, including model poisoning, inference attacks, smart contract exploitation, and consensus manipulation [8, 26, 49, 50]. The comprehensive nature of these cybersecurity challenges highlights the critical need for adaptive, multi-layered defense strategies. These strategies must address the unique characteristics and constraints of IoMT environments while ensuring the reliability and accessibility essential for effective healthcare delivery.

3. Related work

The cybersecurity challenges of IoMT systems have gained significant research interest. Various strategies have been designed to detect, prevent, and mitigate threats. This section offers an overview of the current research in IoMT security. It focuses on ML-based solutions, FL methods, and security frameworks tailored for healthcare environments.

Several studies have established comprehensive taxonomies of IoMT threats and security requirements. Papaioannou et al. [37] provided a detailed overview of attack types and countermeasure strategies in IoMT environments. They systematically mapped threats to the core security objectives of confidentiality, integrity, and availability. Their work highlights the limitations of traditional IT security approaches in protecting medical devices. Complementing this taxonomic approach, Wazid et al. [49] presented a comprehensive survey focusing on malware and botnet attacks in IoMT systems. They provide valuable insights into the evolution of sophisticated threats targeting healthcare infrastructure while reviewing existing detection and prevention protocols. Garg et al. [19] conducted a holistic examination of IoMT security challenges. Their work offers extensive coverage of threats across device, network, and application layers. They emphasize the importance of architectural security through the comprehensive implementation of key management systems, robust authentication protocols, and advanced intrusion detection capabilities [11, 25].

The application of ML techniques to the security of the IoMT has become a prominent research area. Numerous studies have demonstrated the effectiveness of various algorithmic approaches for threat detection and anomaly identification. Recent research has shown particular promise in hybrid deep learning architectures that integrate convolutional neural networks (CNNs) and long short-term

memory (LSTM) networks for detecting edge-centric attacks. Alzubi et al. [4] demonstrate that blended deep learning models significantly enhance detection rates when compared to traditional single-model approaches, particularly in resource-constrained IoMT environments. This emphasizes the significance of computational efficiency in deployment scenarios where device resources are limited. Dhanushkodi et al. [15] presented innovative attention-based LSTM models that demonstrate excellent scalability and generalization capabilities in dealing with multiclass attack scenarios. This addresses the critical need for adaptive algorithms that can evolve with the dynamic IoMT threat landscape. In addition, classical ML approaches have also shown considerable promise, particularly when combined with comprehensive feature engineering. Research has utilized support vector machines (SVM) and k-nearest neighbors (KNN) algorithms, achieving state-of-the-art performance in medical anomaly detection when applied to feature-rich datasets [3, 39].

The sensitive nature of medical data has led to extensive research into FL approaches. These methods allow for collaborative model training while keeping sensitive patient information decentralized and secure. Ahmed et al. [5] explored the integration of physical layer security techniques with FL frameworks, demonstrating that this combination can offer robust collaborative defense mechanisms while preserving patient confidentiality and ensuring healthcare data integrity. Building on this foundation, Barnawi et al. [10] enhanced the research by incorporating differential privacy mechanisms into FL architectures specifically designed for IoMT applications. This integration provides mathematical guarantees for privacy protection and enables effective collaborative threat detection across multiple healthcare institutions. Misbah et al. [30] presented a comprehensive FL framework tailored for IoMT security, which addresses unique challenges such as resource constraints, data privacy, and the heterogeneous behaviors of devices. Their approach utilizes advanced techniques like stacking, federated dynamic averaging, and active user participation. Singh et al. [43] proposed a hierarchical FL architecture that strategically combines dew computing with cloud resources for intrusion detection in IoMT networks. This architecture effectively addresses scalability concerns while maintaining the low-latency requirements that are essential for real-time medical monitoring applications.

Recent research has highlighted the superior performance of ensemble learning methods in the domain of IoMT security applications. Studies consistently indicate that ensemble approaches achieve higher detection accuracy compared to individual algorithms. For instance, Chandekar et al. [13] proposed an ensemble AI-based anomaly detection framework that utilizes the comprehensive CICIoMT2024 dataset. This dataset includes multi-protocol data on Wi-Fi, MQTT, and Bluetooth communications, as well as various attack scenarios, including DoS and DDoS attacks. The effectiveness of ensemble methods, including RF, AdaBoost, and bagging algorithms, has been substantiated by numerous studies. These techniques are helpful in IoMT environments, where the impact of false positives and false negatives can lead to serious operational and safety challenges [45, 48].

An emerging area of research focuses on developing real-time, web-based vulnerability assessment tools that offer actionable insights and automated response capabilities for healthcare cybersecurity professionals. These platforms increasingly incorporate artificial intelligence and ML models to facilitate continuous monitoring, rapid threat diagnosis, and the automated containment of security incidents [7, 11]. Santiago et al. [44] examined how the integration of ML with web intelligence can enhance predictive analytics in cybersecurity applications. Their findings emphasize the possibility of

developing scalable and user-friendly platforms that assist healthcare providers in maintaining robust cybersecurity practices while navigating the complexities of modern IoMT environments.

Blockchain-based trust management systems for IoMT have been increasingly recognized as a strategy to enhance transaction reliability and traceability, while addressing specific attack vectors, including Sybil attacks. Ali et al. [9] proposed the use of Byzantine fault tolerance mechanisms combined with fuzzy logic systems to enhance trust assessment within IoMT networks. Meanwhile, Almalki et al. [7] investigated the broader integration of blockchain technologies with IoMT devices, exploring the potential for distributed ledger systems to offer immutable audit trails and improved data integrity verification in healthcare applications.

The development of comprehensive and realistic benchmark datasets is a crucial advancement in IoMT security research, effectively addressing challenges related to model evaluation and comparison. The introduction of datasets such as IoMT-TrafficData [3] and CICIoMT2024 [14] has enhanced the field by providing multi-protocol network traffic data, a variety of attack scenarios, and extensive device profiling capabilities. These features enable thorough evaluation and comparison of security models. Dadkhah et al. [14] addressed significant gaps in the security research of the IoMT through the introduction of the CICIoMT2024 dataset. This dataset provides comprehensive coverage of various communication protocols, attack types, and device behaviors. It is a vital resource for enabling realistic evaluations of ML-based security solutions.

Although there is considerable research in IoMT security, several critical gaps persist that require further investigation. The performance of ML models is often limited by issues related to data quality, class imbalance, and the computational constraints of resource-constrained IoMT devices. Additionally, data scarcity and the lack of high-quality, publicly accessible IoMT datasets pose challenges for the generalization of proposed solutions across various healthcare environments [27]. The development of lightweight, explainable ML models designed for resource-constrained IoMT settings is an ongoing research priority. Furthermore, the rapid evolution of IoMT technologies, such as the integration of artificial intelligence and edge computing, expands the potential attack surfaces and introduces new security considerations that warrant sustained research focus. Developing adaptive, context-aware security frameworks that can evolve alongside the changing threat landscape remains a critical challenge.

Unlike prior IDS studies that used ensemble techniques mainly on general IoT datasets or single-protocol environments, our approach uniquely integrates RF, AdaBoost, and bagging within a hard voting scheme evaluated on the CICIoMT2024 dataset. This dataset includes Wi-Fi, BLE, and MQTT protocols, enabling a comprehensive and realistic assessment of IoMT-specific security. Furthermore, unlike probability-based fusion rules that dominate prior work, our design employs a deterministic hard voting mechanism with AdaBoost as a tie-breaker. This ensures interpretability and robustness, which are essential for clinical auditing and deployment in regulated healthcare environments.

4. Machine learning models for threat detection

ML has become integral to modern cybersecurity strategies, especially within the IoMT, where traditional rule-based methods struggle due to the heterogeneity and dynamic nature of connected medical devices. Unlike conventional signature-based systems, ML models offer adaptive capabilities, allowing them to analyze historical data, detect previously unseen threats, and operate effectively in

resource-constrained, dynamic IoMT environments.

This study evaluates seven prominent classification algorithms selected for their interpretability, computational efficiency, and demonstrated effectiveness in IoMT cybersecurity research: classification and regression tree (CART), SVM, KNN, RF, naive Bayes (NB), AdaBoost, and bagging. Each algorithm has distinct strengths regarding accuracy, computational demands, and interpretability, making them suitable for integration into the proposed hybrid ensemble methodology.

4.1. Classification and regression tree

The CART algorithm is a common ML method for classification and regression that segments data into branches based on input feature values to predict the target variable. During this process, CART searches for optimal splits that minimize impurity metrics using the Gini impurity index in classification problems and mean squared error (MSE) in regression scenarios. This recursive partitioning divides data into smaller groups, producing decision nodes specifying which feature to split on and terminal leaf nodes that generate predictions.

Specifically, for classification, the Gini index $G(t)$ at a node t is calculated as

$$G(t) = 1 - \sum_{i=1}^{k} p_i^2, \tag{4.1}$$

where p_i stands for the proportion of samples belonging to class i. For regression, the algorithm reduces variability within nodes by minimizing the MSE, given by

$$MSE(t) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})^2, \tag{4.2}$$

where x_i are individual target values, and $\bar{x}$ is their average in the node. The splitting continues recursively until meeting stopping conditions such as limited tree depth or minimal sample count per node. CART's strengths lie in its interpretability and straightforward structure, although it is susceptible to overfitting. To counteract this, pruning techniques; ike cost-complexity pruning, and ensemble methods, such as boosting, are frequently applied to enhance model generalization. In domains such as IoMT security, CART offers valuable transparency, often augmented by ensemble approaches to bolster performance [16, 32, 35, 54].

4.2. Support vector machine (SVM)

SVM constitutes a widely used ML method primarily aimed at classification problems. The core concept involves identifying a hyperplane that distinctly separates data points of different categories while maximizing the margin, defined as the nearest distance between the hyperplane and the closest critical samples known as support vectors. In the simplest two-dimensional scenario, this division is represented by a decision function

$$f(x) = w \cdot x + b, \tag{4.3}$$

where w symbolizes the weight vector determining orientation, x represents the input feature vector, and b indicates the bias term adjusting the boundary's position. Classification results from evaluating

the sign of this function, assigning points with $f(x) > 0$ to one class and those with $f(x) < 0$ to the other.

The optimization problem for SVM is formulated as

$$\min \frac{1}{2}\|w\|^2 \tag{4.4}$$

subject to constraints ensuring all training points (x_i, y_i) satisfy

$$y_i(w \cdot x_i + b) \geq 1, \tag{4.5}$$

where y_i denotes the actual class label. When data are not linearly separable in the original feature space, kernel methods are employed to implicitly project them into higher-dimensional spaces, facilitating linear separation. The SVM demonstrates robust capability in managing complex, high-dimensional datasets typical in IoMT applications, although success hinges on meticulous parameter tuning and sufficient computational power [28, 34].

4.3. K-Nearest neighbors (KNN)

The KNN algorithm is a popular ML method that determines the label or output of a new data point by examining its nearest neighbors in feature space. For classification, KNN assigns the most common class among the nearest k points, whereas for regression it calculates the predicted value by averaging the target values of these neighbors.

Given a new instance x_{new}, the algorithm computes distances to all training points using a metric such as Euclidean distance

$$d(x_{\text{new}}, x_i) = \sqrt{\sum_{j=1}^{d}(x_{\text{new},j} - x_{i,j})^2}, \tag{4.6}$$

where d denotes the number of features, and $x_{\text{new},j}$, $x_{i,j}$ correspond to the j-th features of the test and training points, respectively. Then, the k nearest points are identified. The predicted class for classification is

$$y_{\text{new}} = \text{majority}(y_1, y_2, \ldots, y_k), \tag{4.7}$$

and for regression is

$$y_{\text{new}} = \frac{1}{k}\sum_{i=1}^{k} y_i, \tag{4.8}$$

where y_i represent the labels or target values of the closest neighbors. Notably, KNN is a non-parametric technique that does not assume any prior distribution of the data, contributing to its flexibility. However, this characteristic also leads to considerable computational cost during inference, especially in high-dimensional or large-scale datasets, such as those encountered in IoMT environments. Additionally, the algorithm's performance can be adversely affected by irrelevant or improperly scaled features [52].

4.4. Random forest (RF)

RF is a universal ensemble learning method primarily applied to both classification and regression problems. The algorithm functions by generating numerous decision trees during the training phase, each constructed from bootstrap samples, random subsets of the original dataset sampled with replacement, to instill variability among trees. This randomness enhances the model's generalization capabilities. Moreover, when splitting nodes within a tree, RF considers only a random subset of features rather than the entire set, thereby further reducing correlations among trees and mitigating overfitting.

For classification, the final output corresponds to the class label receiving the majority vote from all trees

$$y_{\text{new}} = \text{majority}(y_1, y_2, \ldots, y_t), \tag{4.9}$$

whereas in regression tasks, the prediction is derived by averaging the outputs of all trees:

$$y_{\text{new}} = \frac{1}{t}\sum_{i=1}^{t} y_i. \tag{4.10}$$

The strength of RF lies in its inherent robustness against overfitting when compared to individual decision trees. Furthermore, RF is suitable for handling large datasets featuring high dimensionality. Key hyperparameters to consider include the number of trees t and the number of features selected for each node split. Additionally, RF provides feature importance metrics, offering insights into the predictive value of each attribute within the model.

RF provides robust performance, effectively handles noisy and heterogeneous IoMT data, and offers valuable feature importance metrics. However, its computational complexity may pose challenges in constrained IoMT settings [42].

4.5. Naive Bayes (NB)

NB is a straightforward yet powerful probabilistic classifier grounded in Bayes' theorem. It operates under the key premise that input features are conditionally independent given the target class, a simplification that gives the algorithm its "naive" label. Despite this strong assumption, which is often violated in practical datasets, NB tends to deliver robust classification results. Bayes' theorem mathematically defines the posterior probability of a class C given a feature vector X as

$$P(C|X) = \frac{P(X|C)P(C)}{P(X)}, \tag{4.11}$$

where $P(C|X)$ is the posterior probability, $P(X|C)$ denotes the likelihood of observing X given class C, $P(C)$ is the prior probability of the class, and $P(X)$ is the evidence or marginal likelihood of the feature vector. The crucial simplification in NB is that the joint likelihood decomposes into a product over individual features

$$P(X|C) = \prod_{i=1}^{n} P(x_i|C), \tag{4.12}$$

where x_i denotes each feature component and n their total count. For classification, NB computes posterior probabilities for all classes, assigning the input to the class $\widehat{C}$ with the highest probability

$$\widehat{C} = \arg\max_{C} P(C) \prod_{i=1}^{n} P(x_i|C). \tag{4.13}$$

NB provides high computational efficiency and scalability, making it ideal for resource-constrained environments such as the IoMT. However, its performance can be affected by strong correlations among input features [51].

4.6. Adaptive boosting

Adaptive boosting (AdaBoost) is an ensemble methodology designed to improve classification accuracy by aggregating multiple weak classifiers into a single, more robust model. It operates through a sequential training process where each successive weak learner concentrates on the training instances misclassified by its predecessors.

Initially, the algorithm assigns an equal weight to every training example, denoted as

$$D_i^{(1)} = \frac{1}{N}, \tag{4.14}$$

where N is the number of samples and $D_i^{(1)}$ the initial weight of the i-th data point.

At iteration t, a weak classifier $h_t(x)$ is trained using the weighted dataset, and its weighted error rate is computed as

$$\epsilon_t = \sum_{i=1}^{N} D_i^{(t)} \cdot \mathbb{I}(h_t(x_i) \neq y_i) \tag{4.15}$$

with $\mathbb{I}(\cdot)$ the indicator function identifying misclassifications.

The importance of the weak learner within the ensemble is then quantified by

$$\alpha_t = \frac{1}{2} \ln\left(\frac{1-\epsilon_t}{\epsilon_t}\right), \tag{4.16}$$

which assigns higher weights to more accurate classifiers.

Subsequently, the weights of the individual training samples are updated to prioritize those incorrectly predicted using the rule

$$D_i^{(t+1)} = D_i^{(t)} \cdot \exp\left(-\alpha_t \cdot y_i \cdot h_t(x_i)\right), \tag{4.17}$$

thus increasing focus on difficult cases and reducing attention on correctly classified points.

The final prediction after T iterations is obtained by the weighted sign aggregation of all weak learners

$$H(x) = \text{sign}\left(\sum_{t=1}^{T} \alpha_t h_t(x)\right), \tag{4.18}$$

where the sign function produces the predicted class label by evaluating the combined influence of constituent classifiers.

AdaBoost improves the performance of weak classifiers by focusing on difficult cases. However, it can be sensitive to noisy data and outliers, requiring careful data preprocessing in IoMT applications [21].

4.7. Bootstrap aggregating (bagging)

Bootstrap aggregating, commonly known as bagging, is an ensemble strategy aimed at enhancing the prediction accuracy and stability of ML models by merging multiple base learners. This technique involves generating numerous training datasets via bootstrap sampling, each created by randomly drawing data points from the original set with replacement, resulting in samples of the same size but varying compositions. Subsequently, independent models are trained on each bootstrapped dataset.

For inference, the outputs of these individual models are consolidated

- In regression problems, by averaging predictions:

$$y_{\text{pred}} = \frac{1}{M} \sum_{i=1}^{M} y_i. \tag{4.19}$$

- In classification tasks, by selecting the class receiving the majority vote among the model outputs

$$y_{\text{pred}} = \text{majority}(y_1, y_2, \ldots, y_M). \tag{4.20}$$

The principal merit of bagging lies in its ability to decrease variance inherent in models with high instability, such as decision trees, thereby mitigating overfitting and improving generalization performance through the diversification of training data subsets [23].

5. Hybrid threat detection model

While individual ML classifiers have been effective for specific cybersecurity tasks, they often struggle to fully comprehend the complexity of IoMT traffic. The diverse range of devices, protocols, and data patterns complicates the detection of security threats. To strengthen our cybersecurity, we need comprehensive solutions that address the evolving risks of IoMT communications and enhance healthcare system security. We introduce an innovative hybrid model that leverages the predictive power capabilities of three complementary algorithms: RF, AdaBoost, and bagging. By strategically integrating these methods, we can significantly enhance accuracy and robustness in our predictions. Our hybrid model utilizes a hard voting technique to finalize predictions. In this method, each base classifier casts a vote, and the class receiving the majority of votes is chosen as the output. This approach guarantees reliable and stable performance by utilizing the combined power of multiple classifiers.

This architecture is well-suited for the dynamic and high-stakes environment of medical systems, where detection accuracy must be balanced with model interpretability and computational efficiency. The proposed hybrid model effectively balances sensitivity and generalization by aligning various learning behaviors under a unified decision protocol. Although conceptually simple, this fusion addresses critical gaps in protocol-specific threat detection and enhances the system's capacity to generalize across various IoMT attack scenarios, providing a practical advancement toward resilient healthcare cybersecurity. Many existing ensemble methods typically depend on probability-based fusion, which can struggle when model outputs conflict or confidence levels are skewed. In contrast, the hard voting strategy presented in our hybrid model guarantees deterministic and interpretable decisions. This design offers a lightweight yet highly accurate solution for threat detection systems,

where reliability and transparency are essential, particularly in healthcare infrastructure subject to strict operational and regulatory requirements.

Let $x_i \in \mathbb{R}^n$ be an input instance. We define three trained classifiers: h_{RF}, h_{AB}, and h_{BG}, corresponding to RF, AdaBoost, and bagging, respectively. Each classifier produces a predicted class label, denoted by $y_j \in \mathcal{Y} = \{0, 1, \ldots, K-1\}$, where K is the total number of classes. In this study, we consider three classification tasks, each with a different number of class labels.

The hybrid model uses a hard voting scheme to make the final prediction. In this scheme, each classifier casts one vote for its predicted class, and the class that receives the majority of votes is selected as the final output. This approach prioritizes model agreement over probability estimates, enhancing interpretability and robustness. The process begins by collecting the individual predictions from the three classifiers as follows

$$y_{\text{RF}} = h_{\text{RF}}(x_i), \quad y_{\text{AB}} = h_{\text{AB}}(x_i), \quad y_{\text{BG}} = h_{\text{BG}}(x_i). \tag{5.1}$$

We then define a vote count vector $V \in \mathbb{Z}^K$, where each element $V[k]$ denotes the number of votes received by class k. The vector is initialized with all entries set to zero:

$$V = [0, 0, \ldots, 0] \quad (\text{length } K). \tag{5.2}$$

Each classifier casts a vote for its predicted class by incrementing the corresponding element in the vote vector:

- Add one vote to the class predicted by RF: $V[y_{\text{RF}}] \leftarrow V[y_{\text{RF}}] + 1$;
- Add one vote to the class predicted by AdaBoost: $V[y_{\text{AB}}] \leftarrow V[y_{\text{AB}}] + 1$;
- Add one vote to the class predicted by Bagging: $V[y_{\text{BG}}] \leftarrow V[y_{\text{BG}}] + 1$.

Once voting is complete, we compute the highest number of votes received by any class:

$$M = \max_{k \in \mathcal{Y}} V[k]. \tag{5.3}$$

We then identify all classes that received this maximum number of votes by constructing the candidate set:

$$\text{candidates} = \{k \in \mathcal{Y} \mid V[k] = M\}. \tag{5.4}$$

The final predicted class label $\hat{y}_i$ is determined based on the size of the candidate set. If there is only one candidate (i.e., no tie), the prediction is set to that class:

$$\hat{y}_i = \text{candidates}[0]. \tag{5.5}$$

Otherwise, if a tie occurs (i.e., multiple classes share the maximum vote count), we default to AdaBoost's prediction:

$$\hat{y}_i = y_{\text{AB}} \tag{5.6}$$

AdaBoost is chosen as the tie-breaker based on its strong empirical performance and generalization ability, especially in edge cases. The decision rule can be summarized as

$$\hat{y}_i = \begin{cases} \arg\max_{k \in \mathcal{Y}} V[k], & \text{if } |\text{candidates}| = 1; \\ y_{\text{AB}}, & \text{otherwise.} \end{cases} \tag{5.7}$$

This procedure defines the final prediction of our hybrid ensemble model. The complete voting process is formalized in Algorithm 1, which outlines the integration of the three classifiers into the hybrid decision system. An overview of the model architecture is illustrated in Figure 1.

Algorithm 1 Hybrid threat detection using hard voting with AdaBoost tie resolution

Require: Test instance x_i, Trained classifiers $h_{\text{RF}}, h_{\text{AB}}, h_{\text{BG}}$, Number of classes K
Ensure: Predicted class label $\hat{y}_i$

Initialize vote vector $V = [0, 0, \ldots, 0]$ of length K
Predict $y_{\text{RF}} \leftarrow h_{\text{RF}}(x_i)$
Predict $y_{\text{AB}} \leftarrow h_{\text{AB}}(x_i)$
Predict $y_{\text{BG}} \leftarrow h_{\text{BG}}(x_i)$
Add one vote to class y_{RF}
Add one vote to class y_{AB}
Add one vote to class y_{BG}
Let $M \leftarrow \max(V)$
Let candidates $\leftarrow \{k \mid V[k] = M\}$
if |candidates| = 1 **then**
    $\hat{y}_i \leftarrow$ the single element in candidates
else
    $\hat{y}_i \leftarrow y_{\text{AB}}$ ▷ Use AdaBoost in case of tie
end if
return $\hat{y}_i$

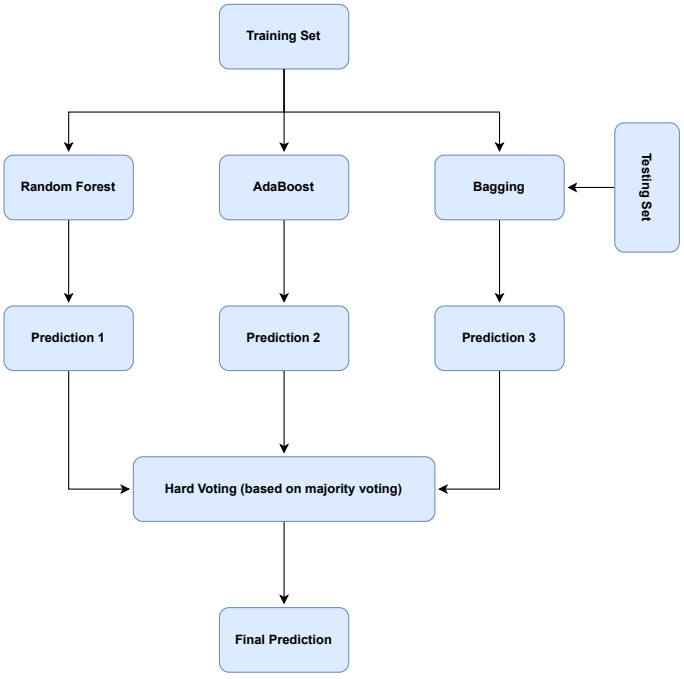

Figure 1. Architecture of the hybrid threat detection model.

This approach enables the hybrid model to make consistent and predictable decisions, even in uncertain situations. By integrating the unique strengths of three powerful classifiers: RF for its exceptional robustness, bagging for its effective variance reduction, and AdaBoost for its ability to target challenging classifications, this voting-based hybrid model boosts generalization and reduces false positive rates. The result is a more accurate and reliable model that can confidently tackle complex classification challenges. It is particularly well-suited for IoMT environments, where the traffic is diverse and the threat profiles vary across communication protocols. This design also provides a reliable and generalizable framework for threat detection in IoMT systems, effectively addressing the limitations of single-model predictions. It offers a scalable and easily deployable solution that enhances the field of ensemble learning in crucial areas like healthcare cybersecurity.

The proposed hybrid model offers three key benefits that improve its effectiveness for real-world implementation in IoMT threat detection. The system achieves resilience at the protocol level by utilizing the complementary strengths of its underlying classifiers. RF effectively captures structured patterns in Bluetooth traffic, while AdaBoost is reliable in imbalanced settings commonly seen in MQTT-based communication. This variety enables the proposed hybrid model to generalize across all protocols in the CICIoMT2024 dataset. The hybrid model also reduces false positive rates. While individual classifiers may misclassify unusual or borderline cases, the voting mechanism helps correct these errors by strengthening agreement among models. This improvement is particularly critical in healthcare environments, where false alarms can lead to unnecessary operational responses and may put patient safety at risk. The hybrid model stands out with its scalability and ability to generalize effectively, making it a powerful choice for various applications. It retains high accuracy not only on known attack types, but also on new threats, demonstrating its strength against evolving attack surfaces and complex, real-time traffic scenarios.

Additionally, the hybrid model is designed for efficiency, achieving high accuracy without significant computational overhead. It can operate in near-real-time, making it suitable for integration into continuous monitoring systems in hospitals and medical facilities. The experimental results presented in Section 6.4 validate its superiority over single classifiers in predictive performance and operational reliability, reinforcing its value as a comprehensive threat detection solution for modern IoMT ecosystems.

6. Experimental analysis

In this section, we present the experimental framework designed to rigorously evaluate the effectiveness of the proposed hybrid threat detection model. We begin by describing the benchmark dataset used in this study, highlighting its relevance and complexity in the context of IoMT cybersecurity. Next, we outline the experimental setup, detailing the implementation environment and methodological procedures. We then introduce the evaluation metrics used to assess and compare model performance. Finally, we report and analyze the experimental results, demonstrating the hybrid model's superiority over baseline classifiers and discussing its implications for real-world deployment.

6.1. The CICIoMT2024 dataset

A high-quality, domain-specific dataset is crucial for developing effective ML models in the field of IoMT security. In this study, the CICIoMT2024 dataset [14], provided by the Canadian Institute

for Cybersecurity, serves as the primary benchmark for model development and evaluation. Designed explicitly for anomaly detection in IoMT environments, CICIoMT2024 addresses key limitations of previous datasets by incorporating a wide range of communication protocols, device types, and attack scenarios. Its structure includes multi-protocol data, device attack-specific data, time-series data, and device-specific profiles, providing the depth and diversity necessary for training and evaluating ML models under realistic and varied conditions. This makes CICIoMT2024 particularly well-suited to achieve the objectives of this research.

The CICIoMT2024 dataset captures network traffic from a variety of IoMT devices, including sensors, wearables, and smart medical equipment, operating across heterogeneous communication protocols such as Wi-Fi, BLE, and MQTT. This diversity of protocols allows for a realistic simulation of healthcare environments and introduces the necessary variability critical for developing models that do not rely on specific protocols.

The CICIoMT2024 dataset contains both benign and malicious traffic samples, with the latter including a wide range of cyberattack types. Specifically, the dataset encompasses five major attack categories: DoS, DDoS, reconnaissance, MQTT-based attacks, and spoofing. These five attack categories represent distinct threat vectors commonly encountered in IoMT environments. DoS attacks share similar objectives but originate from a single source, typically targeting a specific device or service to disrupt its availability. DDoS attacks involve coordinated flooding attempts from multiple sources, aiming to overwhelm a target system or network infrastructure. Reconnaissance attacks focus on information gathering through techniques such as port scanning, OS fingerprinting, and network probing to uncover vulnerabilities. MQTT-based attacks exploit weaknesses in the lightweight messaging protocol widely used in IoMT, including publish/subscribe flooding and injection of malformed packets. Spoofing attacks involve the impersonation of legitimate devices, such as ARP spoofing, to intercept, redirect, or manipulate network traffic. These types of attacks represent a wide range of adversarial behaviors that are crucial for assessing the robustness of ML models in healthcare cybersecurity. Each attack category is further divided into multiple attack variants, resulting in a total of 18 distinct class labels. This multi-class framework allows for detailed classification tasks and facilitates performance evaluation across various threat scenarios.

The CICIoMT2024 dataset includes 44 numerical features derived from network traffic flows, capturing key behavioral and structural characteristics essential for anomaly detection. These features encompass metrics such as packet size distribution, inter-arrival time, protocol-specific flags, and transport-layer indicators, offering a comprehensive view of both statistical and protocol-level patterns. A complete summary of these features is presented in Table 1. This level of detail enables ML models to identify subtle differences associated with complex and multifaceted IoMT attacks. For experimental analysis, the class variable in the dataset can be interpreted in three distinct ways. First, it can be considered a binary classification task that differentiates between benign traffic and attack traffic. Alternatively, it can be viewed as a multi-class classification task that includes benign traffic along with five main attack categories. Lastly, the variable can be analyzed as a detailed multi-class classification task involving 19 classes, encompassing benign traffic and the various 18 attack subtypes. A brief description of these 18 attack subtypes is shown in Table 2. This flexibility supports various evaluation scenarios, ranging from general threat detection to highly detailed attack classification.

Due to its scale, diversity, and high-fidelity simulation of IoMT environments, the CICIoMT2024 dataset is a rigorous and appropriate benchmark for evaluating the performance and generalization

capabilities of the proposed hybrid ensemble model. It encourages meaningful experimentation across imbalanced, multi-protocol, and multi-class conditions commonly encountered in healthcare cybersecurity settings.

Table 1. Features description of the CICIoMT2024 dataset [31].

Feature	Description	Feature	Description
Header Length	Packet header length	Duration	Packet lifetime in transit
Rate	Packet transmission speed	Srate	Speed of outgoing packets
Tot sum	Total packet length	Tot size	Total packet size
Min	Minimum packet length	Max	Maximum packet length
AVG	Average packet length	Std	Packet length variability
IAT	Interval between packets	Number	Total packets in flow
Radius	RMS of variances of lengths	Magnitude	RMS of averages of lengths
Variance	Variance ratio of lengths	Covariance	Covariance of packet lengths
Weight	Product of packet counts	Protocol Type	Protocol type as integer
Fin flag number	TCP/IP Fin flag value	Syn flag number	TCP/IP Syn flag value
Rst flag number	TCP/IP Rst flag value	Psh flag number	TCP/IP Psh flag value
Ack flag number	TCP/IP Ack flag value	Ece flag number	TCP/IP Ece flag value
Cwr flag number	TCP/IP Cwr flag value	Fin count	Fin flag occurrences
Syn count	Syn flag occurrences	Ack count	Ack flag occurrences
Rst count	Rst flag occurrences	HTTP	Indicates HTTP usage
HTTPS	Indicates HTTPS usage	DNS	Indicates DNS usage
Telnet	Indicates Telnet usage	SMTP	Indicates SMTP usage
SSH	Indicates SSH usage	IRC	Indicates IRC usage
TCP	TCP in transport layer	UDP	UDP in transport layer
DHCP	Indicates DHCP usage	ARP	ARP in link layer
ICMP	ICMP in network layer	IGMP	Indicates IGMP usage
IPv	IP in network layer	LLC	LLC in link layer

Table 2. Summary of attack types in the CICIoMT2024 dataset [53].

Class	Attack name	Protocol	Description/Target
Spoofing	ARP Spoofing	Wi-Fi	MITM, ARP cache poisoning
Recon	Ping Sweep	Wi-Fi	Host enumeration
Recon	VulScan	Wi-Fi	Vulnerability scanning
Recon	OS Scan	Wi-Fi	Identify OS fingerprint
Recon	Port Scan	Wi-Fi	Identify open ports/services
MQTT	Malformed Data	MQTT	Broker/protocol abuse
MQTT	DoS Connect Flood	MQTT	Single-source session abuse
MQTT	DDoS Connect Flood	MQTT	Multi-source session abuse
MQTT	DoS Publish Flood	MQTT	Single-source publish abuse
MQTT	DDoS Publish Flood	MQTT	Multi-source publish abuse
DoS	TCP Flood	Wi-Fi	TCP resource exhaustion
DoS	ICMP Flood	Wi-Fi	ICMP bandwidth exhaustion
DoS	SYN Flood	Wi-Fi	Half-open TCP floods
DoS	UDP Flood	Wi-Fi	UDP bandwidth exhaustion
DDoS	DDoS SYN Flood	Wi-Fi	Distributed SYN attack
DDoS	DDoS TCP Flood	Wi-Fi	Distributed TCP attack
DDoS	DDoS ICMP Flood	Wi-Fi	Distributed ICMP attack
DDoS	DDoS UDP Flood	Wi-Fi	Distributed UDP attack

6.2. Experimental setup

All experiments in this study were conducted using the R programming environment, a robust platform for data analysis, ML, and performance evaluation. The computational setup consisted of a Mac running macOS Sequoia 15.5, with R version 4.4.3 (2025-02-28) and RStudio 2024.12.1 (Build 563, "Kousa Dogwood" release). The CICIoMT2024 dataset was initially cleaned by removing duplicate records to eliminate redundancy that could bias the learning process and hinder model generalization.

An 80/20 train-test split was used, with 80% for training and 20% for testing. The test set was strictly held out during training and tuning to ensure that performance metrics reflect generalization to unseen data. This ratio split is widely regarded as a practical and effective rule of thumb for handling large datasets; it provides sufficient data for adequate learning while retaining a statistically meaningful test set for unbiased evaluation [38].

While k-fold cross-validation is a common strategy for performance estimation, we selected a static 80/20 train-test split due to the large scale and diversity of the CICIoMT2024 dataset. To ensure the integrity of this approach, the partition was created using stratified sampling. This crucial step ensures that all classes are accurately represented, from benign traffic to each specific attack category, in both the training and testing sets. This stratification ensures that our hold-out test set accurately represents the overall data distribution, effectively addressing concerns about sampling bias and ensuring the stability of the results. Given that this representative test set is already statistically significant in size, it provides a reliable estimate of the model's generalization performance, thus achieving the core objectives of cross-validation without the excessive computational overhead of repeatedly training the

model across multiple folds.

To enhance model training equality and improve algorithmic stability, all numerical attributes were standardized. All features were standardized to have a mean of 0 and a standard deviation of 1. This step ensures that features with larger numeric ranges do not overly influence the learning process, enhancing the convergence behavior of various ML algorithms. Initially, we explored feature selection through correlation analysis and recursive feature elimination techniques. These approaches failed to yield any significant enhancement in the models' performance. As a result, all 44 numerical features were kept for the training process. This decision guarantees that no potentially informative attribute is discarded and leverages the model's inherent ability to manage high-dimensional input data effectively.

The experimental evaluation was organized into three distinct classification scenarios based on the definition of the class variable. These scenarios are summarized in Table 3. This multi-scenario design allows for a thorough performance assessment, ranging from general anomaly detection in binary cases to detailed classification of specific threat types in a multi-class setting.

Table 3. Class variable scenarios for model evaluation.

Scenario	No. of Classes	Description
1	2	Binary classification: Benign + Attack
2	6	Multi-class classification: Benign + 5 major attack categories (DoS, DDoS, Spoofing, Recon, MQTT)
3	19	Detailed multi-class classification: Benign + 18 specific attack subtypes

6.3. Model performance evaluation metrics

To evaluate the effectiveness of a threat detection system, particularly in critical environments such as IoMT-based healthcare networks, we need metrics that reflect not only overall accuracy, but also the system's reliability in identifying both threats and normal traffic. Misclassifications, whether they result in false alarms or missed attacks, can lead to serious operational and safety consequences. Thus, we concentrate on four widely recognized evaluation metrics: accuracy, precision, recall, and F1-score. These metrics reflect various aspects of model performance and provide a comprehensive overview of predictive quality.

We start by defining the essential components of a confusion matrix used in binary classification.

- True Positive (TP): The classifier correctly identifies an attack instance.
- True Negative (TN): The classifier correctly identifies a benign (non-attack) instance.
- False Positive (FP): The classifier incorrectly labels a benign instance as an attack.
- False Negative (FN): The classifier fails to detect an actual attack.

We define the evaluation metrics as follows:

- Accuracy is the most commonly utilized measure to evaluate the effectiveness of classifiers. It refers to the ratio of correctly classified instances to the total number of instances:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}. \tag{6.1}$$

- Precision is the ratio of correctly predicted positive instances (true positives) to the total number of instances predicted as positive:

$$\text{Precision} = \frac{TP}{TP + FP}. \tag{6.2}$$

- Recall is the ratio of correctly predicted positive instances (true positives) to the total number of actual positive instances:

$$\text{Recall} = \frac{TP}{TP + FN}. \tag{6.3}$$

- F1-score is defined as the harmonic mean of precision and recall:

$$\text{F1-score} = \frac{2TP}{2TP + FP + FN}. \tag{6.4}$$

In multi-class classification, performance evaluation metrics should be aggregated across all classes to accurately reflect overall performance. Macro-averaging is a commonly used method in these situations. In the macro-averaging approach, each metric, such as precision, recall, or F1-score, is calculated independently for every class, and then the arithmetic mean of those values is taken. Macro-averaging treats all classes equally, giving each class the same influence on the final score, regardless of class imbalance. This study employs macro-averaging to evaluate all multi-class metrics. The rationale behind this approach is based on the nature of IoMT threat detection, where some attack categories occur much less frequently than others but are still critically important. By using macro-averaging, we ensure that more common traffic classes do not overshadow rare yet high-risk attack types. This decision results in a more balanced and representative assessment of model performance across a diverse range of threat scenarios.

Overall, adopting accuracy, precision, recall, and F1-score creates a robust and transparent framework for evaluating the effectiveness of our hybrid model. This comprehensive approach not only enhances our understanding of the model's performance, but also ensures that we make informed decisions based on reliable insights. Using macro-averaging in multi-class scenarios provides a comprehensive evaluation of performance that goes beyond just overall accuracy. It also considers consistency across different, and often imbalanced, threat categories. This detailed assessment shows that the model is well-suited for use in real-world IoMT security environments.

6.4. Results and discussion

The hybrid ML model that combines RF, AdaBoost, and bagging was thoroughly evaluated using the CICIoMT2024 dataset, and the results demonstrate its superiority in a variety of performance metrics across different classification scenarios. This hybrid model outperformed individual classifiers, providing more reliable and robust threat detection, which is crucial for securing sensitive IoMT environments, particularly in healthcare.

Figure 2 compares the accuracy, precision, recall, and F1-score of various ML models including CART, SVM, KNN, RF, NB, AdaBoost, bagging, and the proposed Hybrid model, in the detection of threats within binary classes (attack vs. benign) in IoMT traffic. The hybrid model achieves the highest accuracy (99.72%) (Table 4), clearly outperforming individual classifiers such as RF (99.60%) and AdaBoost (99.68%). Precision and recall metrics similarly peak for the hybrid approach, demonstrating its superior ability to avoid both false positives and false negatives. These results are critical for IoMT deployments where the cost of misclassifying threats or raising unwarranted alarms is especially high due to potential patient safety implications.

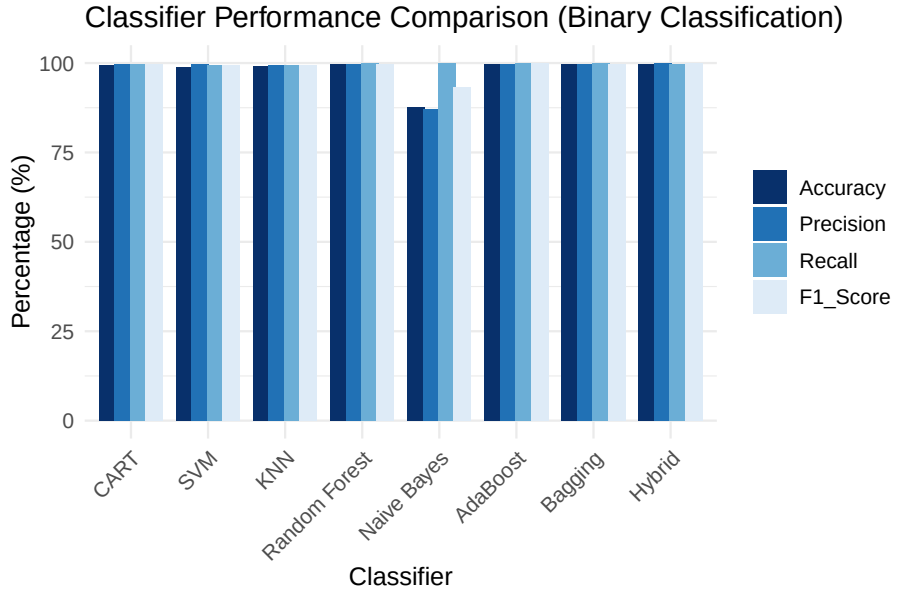

Figure 2. Classifier performance in binary classification (benign vs. attack). The hybrid model achieves the best results across all metrics, minimizing false positives and false negatives in IoMT detection.

Table 4. Performance comparison of models on binary classification (2C).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
CART	99.38	99.73	99.62	99.68
SVM	98.90	99.56	99.29	99.43
KNN	99.04	99.54	99.46	99.50
RF	99.60	99.73	99.85	99.79
NB	87.70	87.15	**99.98**	93.13
AdaBoost	99.68	99.71	99.96	99.83
Bagging	99.58	99.73	99.83	99.78
Hybrid	**99.72**	**99.92**	99.79	**99.85**

This performance trend reflects broader findings in contemporary AI-driven IoMT research, where advanced ensemble and hybrid models repeatedly surpass traditional stand-alone models in both detection efficacy and robustness against attack diversity. Notably, introducing explainable ensemble systems, like the hybrid voting approach, enhances operational transparency, which is vital for trust and regulatory compliance in healthcare environments. Moreover, studies leveraging deep learning hybrids (e.g., CNN-LSTM) for sequential and grid data report accuracy levels consistent with those observed here, highlighting the broader validity and applicability of ensemble constructs in this domain.

Figures 3 and 4 extend the comparative evaluation to more complex, multi-class classification settings. The hybrid approach maintains a decisive advantage, attaining 99.67% accuracy and 98.46% accuracy in 6-class (Table 5) and 19-class (Table 6) tasks, respectively. This sustained high performance across increasing class granularity showcases the model's ability to generalize across diverse IoMT attack types and communication protocols, a necessity for real-life systems where threat

landscapes are multifaceted, involving denial-of-service (DoS/DDoS), spoofing, reconnaissance, and protocol-specific attacks, as summarized in Table 2.

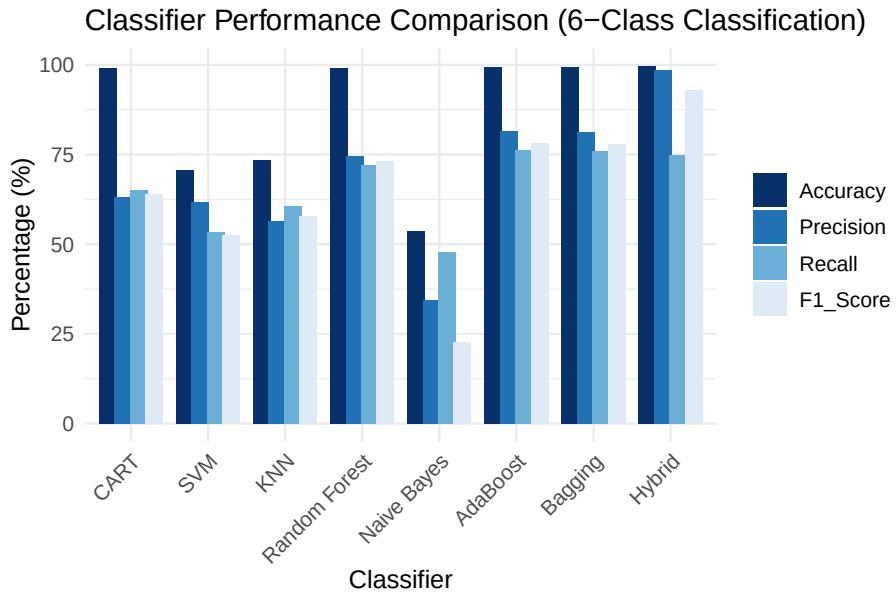

Figure 3. Classifier performance in 6-class classification (benign + 5 attack categories). The hybrid model outperforms all baselines, showing strong generalization across multiple attack types.

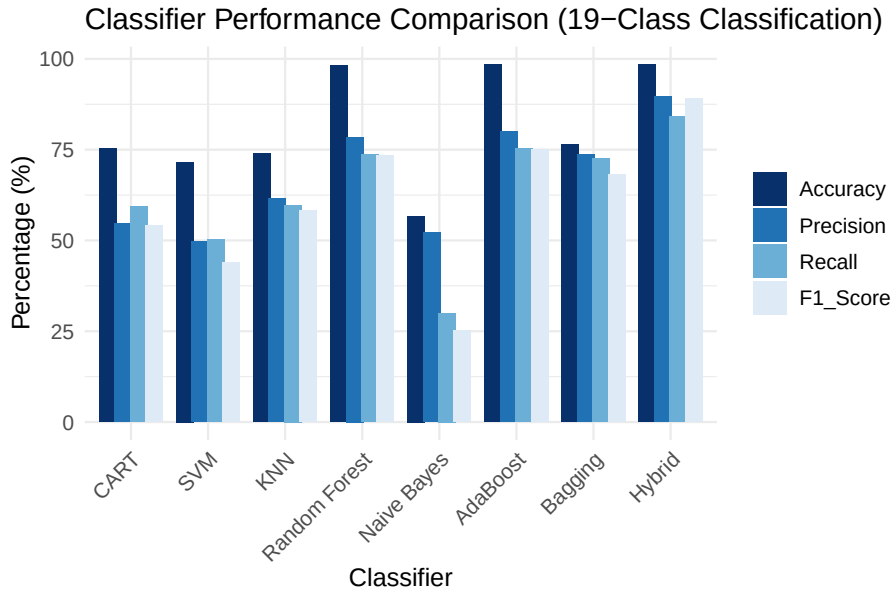

Figure 4. Performance comparison of classifiers in a 19-class classification task. The figure displays key metrics such as accuracy, precision, recall, and F1 score.

Table 5. Performance comparison of models on 6-class classification (6C).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
CART	99.14	63.20	65.02	64.05
SVM	70.53	61.74	53.30	52.68
KNN	73.42	56.52	60.58	57.91
RF	99.20	74.66	72.07	73.09
NB	53.68	34.29	47.82	22.68
AdaBoost	99.46	81.42	**76.26**	78.15
Bagging	99.48	81.17	75.99	77.89
Hybrid	**99.67**	**98.44**	74.90	**92.88**

Table 6. Classifier performance in 19-class classification (benign + 18 attack subtypes). The hybrid model achieves the highest accuracy and F1-score, confirming its reliability in fine-grained threat detection.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
CART	75.34	54.75	59.46	54.22
SVM	71.60	49.70	50.37	43.87
KNN	74.02	61.63	59.77	58.33
RF	98.18	78.50	73.62	73.32
NB	56.73	52.11	30.02	25.27
AdaBoost	98.36	80.12	75.35	75.05
Bagging	76.55	73.59	72.45	68.10
Hybrid	**98.46**	**89.70**	**84.21**	**89.20**

These outcomes align with advances in the literature, where multi-level ensemble learning, FL, and feature-engineering strategies are shown to offset the challenges posed by class imbalance and concept drift in heterogeneous IoMT datasets. Studies employing federated architectures also confirm that decentralized, privacy-aware strategies do not compromise model accuracy, but instead promote scalability and security by leveraging edge computing for prompt local analysis.

To effectively illustrate the comparative performance, we present a radar chart (Figure 5) that captures all four evaluation metrics across the three classification scenarios. This visual representation provides a clear and comprehensive understanding of the performance differences, highlighting the strengths and weaknesses of each scenario. Our proposed hybrid model consistently dominates the chart area in each case, reflecting its balanced and superior performance regardless of classification complexity. This consistency emphasizes the model's suitability for real-time healthcare applications, where maintaining high accuracy is crucial across diverse and unpredictable traffic patterns.

The feature importance plot using the RF algorithm, shown in Figure 6, illustrates the relative significance of various features in determining the model's output. "IAT" (referring to the Interval Between Packets feature) is the most influential variable, with a feature importance score significantly greater than that of the nearest feature. This indicates that it has a significant influence on the predictive models. The significant difference between "IAT" and the other features suggests that this variable plays a vital role in predicting cyberattack types, indicating its substantial impact on the target outcome.

The lower-ranked features are still relevant, but they provide limited predictive insights in this context.

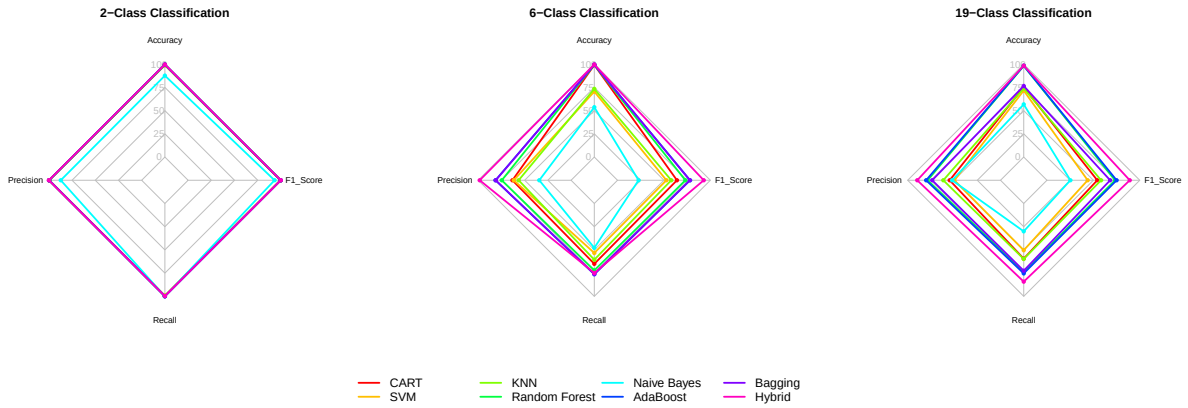

Figure 5. Radar chart of model performance across binary, 6-class, and 19-class tasks. The hybrid model consistently dominates across all metrics, highlighting its robustness.

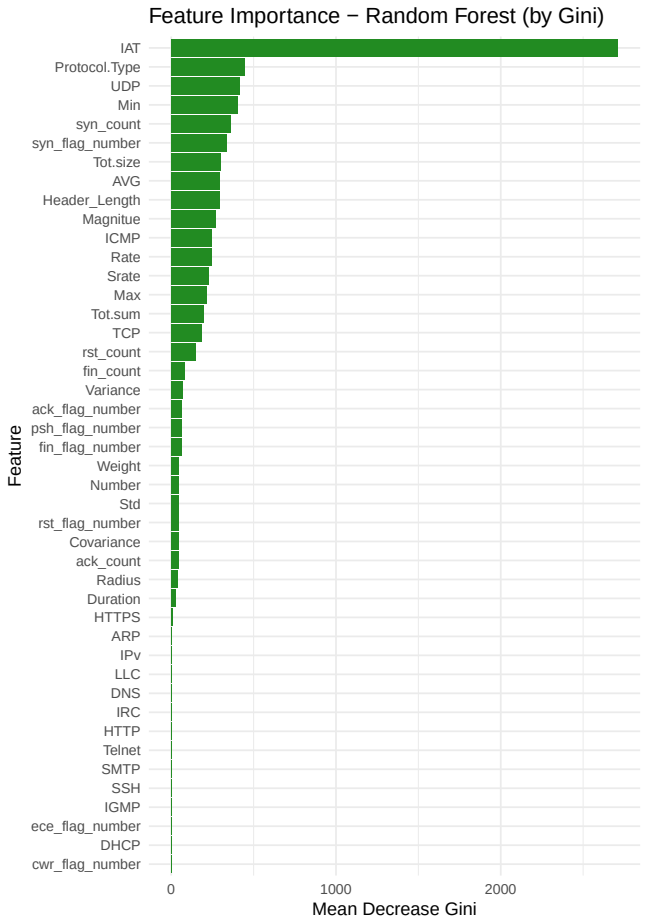

Figure 6. Feature importance ranking using RF. The IAT feature is the most influential, providing interpretability for IoMT traffic analysis.

The bar plots and performance Tables 4–6 collectively demonstrate that the hybrid ensemble not

only increases detection rates, but also significantly reduces false positives, an aspect that is particularly crucial in real-time clinical contexts. High precision (99.92%) and F1 scores (99.85% for binary; above 89% for complex tasks) affirm the system's reliability in distinguishing benign from malicious behaviors without causing unnecessary operational disruptions.

These findings are corroborated by several recent studies that have adopted hybrid IDS frameworks, FL, and blockchain-assisted security to deliver resilient, low-latency, and transparent solutions, often reporting operational improvements and adoption-friendliness in resource-constrained and privacy-sensitive IoMT environments. Additionally, swarm intelligence-based architectures and reinforcement learning, now gaining traction, are shown to further enhance the adaptability and efficiency of intrusion defense in highly dynamic healthcare infrastructures.

Table 7. Comparison of Study Methods, Datasets, Performance, Limitations, and Superiority.

Study	Method & Dataset	Performance Results	Limitations	Why Our Study Is Superior
SafetyMed [17]	CNN-LSTM hybrid IDS evaluated on sequential and grid data (IoMT)	Acc: 97.63% F1: 97.73% Precision: 98.47% Recall: 97%	Evaluated on limited scenarios; architecture is deep and computationally intensive; lacks real-time edge suitability	Achieves ¿99.7% accuracy (binary) and ¿98% (multi-class), operates efficiently on edge, and is interpretable (feature importances, hard voting logic), crucial for real-time medical deployment.
HFL-HLSTM [43]	Hierarchical-Federated LSTM (Dew-Cloud model) using distributed servers	Acc: 99.31% Low training loss	Focus on federated privacy protection; depends on cloud for training; interpretability and explainability not prioritized	Focuses on centralized and edge-ready detection, low computational cost, and improved explainability for robust medical auditing, achieving similar or better accuracy without privacy-leakage risks.
HHO-DRNN [24]	Harris Hawk Optimization with Deep Recurrent NN; optimal feature selection	Acc: 99.85% (outperforms baseline ML/DL)	No discussion of interpretability; computational demands can be high; lacks detail on real-time false alarm control	Our feature importance analysis (RF, CART) and low FPR (as low as 0.8%) specifically target explainable deployments in resource-constrained IoMT, validated on multi-protocol, multi-class settings.
CGAN-CNN IDS [47]	Conditional GAN + CNN; data balancing for imbalanced IDS datasets	F1: 97.88% Precision: 97.15%	Primarily evaluated on general NIDS datasets; not tailored to multi-protocol health IoMT; lacks feature-level interpretability	It achieves higher accuracy and explicitly supports interpretability and protocol diversity .
Swarm-NN IDS [33]	Swarm Intelligence-based Neural Network Edge-centric, ToN-IoT dataset	Acc: 99.5%	Dataset doesn't capture medical multi-protocol heterogeneity; lacks hard false alarm rates; no transparency in decision process	Include rigorous multi-protocol validation and macro-averaged metrics (precision/recall/F1), with top scores (+99.7%), and transparent, explainable logic .
HIDS-IoMT [12]	Hybrid CNN-LSTM, fog-computing, IoTID20/Edge-IIoTset	Acc: 99.92% Precision: 99.91% Recall: 99.99% F1: 99.95%	Requires fog hardware (Raspberry Pi), tested on non-IoMT-specific datasets; scalability, computational resource burden not analyzed	It works on standard clinical edge devices, and is validated for IoMT traffic heterogeneity and multi-class settings, emphasizing low-cost and practical deployment.
Blockchain-Assisted IoMT [8]	Blockchain-based decentralized system; integrated medical data flows	Security rate: 99.8%; latency: 4.3%; reliability: 99.4%	Focus on end-to-end data security, not attack detection granularity; not an ML/IDS framework; no explainability	Our IDS directly addresses intrusion detection with high accuracy and protocol-resolved attack explainability, while blockchain can be complementary but not a substitute for adaptive IDS.

Overall, the hybrid ML model proves to be a scalable, reliable, and effective solution for securing IoMT systems against a wide range of evolving digital threats. The results strongly support its potential

for practical deployment in healthcare networks, where cybersecurity is vital for ensuring the security and privacy of sensitive medical data and patient safety. Its ability to reduce false positives while achieving high accuracy across multiple protocols and classification tasks demonstrates its robustness and suitability for the dynamic and high-stakes environment of modern healthcare systems. Table 7 summarizes a comparison of various studies, including their methods, performance results, limitations, and why the current study is superior.

6.4.1. Summary of superiority and significance

Our study advances the state-of-the-art on several fronts:

- **Empirical performance:** Outperforms recent deep learning, federated, and GAN/Swarm-inspired approaches with up to 99.72% accuracy and 99.92% precision for binary IoMT intrusion detection demonstrating surpassing SafetyMed, CGAN-CNN, and Swarm-NN (Table 4).
- **Practical edge deployment:** Relies on RF, AdaBoost, bagging, enabling real-time operation on constrained medical devices, unlike deep/fog/federated models needing more hardware or cloud/federated actors.
- **Robustness across protocols & classes:** Demonstrated high accuracy not just for binary attacks, but also for 6-class and 19-class multi-protocol scenarios, outperforming state-of-the-art on specificity and generalizability for Wi-Fi, BLE, and MQTT settings.
- **Explainability and auditing:** Explicit feature importance analysis (Figure 6), hard voting, and macro-averaging enable deployment in environments requiring auditability, which is not possible with deep/federated models lacking interpretability.
- **Lower false alarms:** Directly reports precision as high as 99.92%, reducing operational disruption in sensitive healthcare workflows, a metric often missing in prior works.
- **Holistic validation:** Benchmarked thoroughly on CICIoMT2024, a realistic, multi-modal, multi-protocol IoMT dataset, while many previous models test on synthetic or narrow datasets.
- **Clinical applicability:** Provides a comprehensive, scalable, and transparent solution that is directly relevant to practitioners, security officers, and auditors in healthcare, addressing core needs identified in recent reviews.

7. Conclusions and future work

This study proposes a comprehensive hybrid ML framework to address critical cybersecurity challenges faced by the IoMT networks. The research integrates three distinct ML models, RF, AdaBoost, and bagging, into a unified ensemble approach. The model achieves outstanding detection accuracy, with an impressive precision rate of 99.92% and very low false-positive rates, making it a reliable and efficient solution for identifying malicious traffic in healthcare environments. This level of accuracy is particularly crucial in medical settings, where false alarms can disrupt patient care and workflow, and missed detections can have dire consequences.

The proposed hybrid framework is rigorously validated using the CICIoMT2024 dataset, which accurately simulates real-world IoMT traffic scenarios across multiple communication protocols, including Wi-Fi, BLE, and MQTT. The system demonstrates superior performance in comparison to existing state-of-the-art methods, providing a comprehensive solution for IoMT cybersecurity that accounts for both the complex attack vectors and the resource constraints typical in medical devices.

Our framework shows a significant improvement in detection performance over traditional methods, especially in handling diverse and sophisticated cyberattacks targeting IoMT systems. It addresses key security concerns such as device spoofing, DoS attacks, and protocol-specific vulnerabilities, ensuring that healthcare operations remain secure and uninterrupted. The proposed approach proves to be highly effective in safeguarding sensitive medical data while maintaining operational integrity, which is essential in real-time medical environments.

Building on the work presented, a primary direction for our future research will be a comprehensive computational performance analysis. This will involve benchmarking the model's inference time, memory footprint, and energy consumption on various resource-constrained hardware platforms to optimize it for real-time deployment in live IoMT networks.

While the proposed hybrid ML framework demonstrates strong performance, several avenues remain for future research and improvements, particularly in enhancing scalability, privacy, and adaptability to evolving IoMT threats.

1) Scalability for large-scale deployments: One important area for future development is improving the scalability of the model to accommodate large-scale IoMT systems. As healthcare facilities increasingly deploy a wide variety of interconnected devices, the model must be capable of handling the massive volume of data generated by these devices. The hybrid model's computational efficiency, especially in resource-constrained environments, is essential for real-time deployment, but further optimizations will be needed to ensure its effectiveness in larger, more complex networks.

2) FL for privacy and efficiency: Given the sensitive nature of medical data, a promising direction for future work is the incorporation of FL into the hybrid framework. FL allows for the collaborative training of models across distributed devices without the need for centralized data collection, thereby preserving the privacy of sensitive patient information. This decentralized approach can reduce the computational burden on edge devices, making the system more efficient while maintaining strict data privacy standards, which is a critical requirement in healthcare applications.

3) Integration of deep learning techniques: While ensemble methods like RF, AdaBoost, and bagging provide excellent performance, deep learning methods have shown great promise in cybersecurity and anomaly detection. Future work could explore integrating deep learning models such as CNNs and LSTM networks to capture more complex, sequential attack patterns. These models can help address emerging threats in IoMT environments, particularly in scenarios where attacks evolve dynamically and cannot be detected using traditional methods [46].

4) Lightweight models for resource-constrained devices: Many IoMT devices have limited computational power, which poses a challenge for deploying complex ML models. To address this limitation, future research should focus on developing lightweight models that retain high detection accuracy while minimizing computational costs. By optimizing the hybrid model for resource-constrained devices, it can be made suitable for a wider range of medical devices, from low-power wearables to more sophisticated diagnostic equipment.

5) Continuous learning and adaptation to new threats: The cybersecurity landscape is continuously evolving, and IoMT systems must adapt to emerging threats. Future work could explore techniques for continuous learning within the proposed hybrid model. This would enable the system to adapt in real-time to new attack vectors without requiring frequent retraining. Approaches such as online learning or reinforcement learning could be employed to ensure that the model can quickly adapt to previously unseen attack scenarios, thus enhancing the model's ability to deal with novel and sophisticated cyber

threats.

6) Enhancing feature engineering and attack detection granularity: Future research should focus on advanced feature engineering techniques to further enhance the detection capabilities of the hybrid model. By incorporating additional features from the underlying network traffic, such as deeper protocol-level insights or device-specific behaviors, the model's accuracy in detecting complex attack scenarios can be improved. Additionally, fine-tuning the granularity of attack detection, moving from binary detection to more detailed categorization of attack types (e.g., DoS, DDoS, spoofing, reconnaissance), could enhance the system's ability to distinguish between different attack vectors, providing more actionable insights for healthcare security teams.

7) Integration with blockchain for data integrity and auditing: A promising future avenue involves the integration of blockchain technology with the hybrid ML model. Blockchain can provide a decentralized, immutable ledger for tracking IoMT network activities, which would enhance data integrity, ensure secure audit trails, and protect against tampering. Combining the detection capabilities of ML models with blockchain's transparency could offer a powerful, multi-layered security solution for IoMT environments, particularly for monitoring sensitive medical data. [2]

8) Real-world testing and broader dataset expansion: To further validate the practical applicability of the proposed model, future research should focus on real-world testing across diverse healthcare environments and expanding the evaluation dataset. The CICIoMT2024 dataset, while extensive, is still limited in terms of its diversity of devices and attack scenarios. A broader range of IoMT devices, including new and emerging technologies, as well as more diverse real-world attack scenarios, would provide a more comprehensive test for the system's robustness and generalization capabilities.

By addressing these areas, future iterations of the hybrid ML framework can evolve into a highly scalable, adaptable, and privacy-preserving cybersecurity solution suitable for the rapidly growing and complex IoMT ecosystem.

This study paves the way for more effective and secure IoMT systems by demonstrating how advanced machine learning techniques can be tailored to meet the unique security challenges of healthcare environments. As the IoMT continues to grow and evolve, this hybrid approach offers a foundation for ongoing improvements in cybersecurity, ensuring that patient safety and sensitive medical data remain protected from increasingly sophisticated cyber threats.

Author contributions

Abdulmajeed Atiah Alharbi: Conceptualization, methodology, software, validation, formal analysis, writing-review and editing, visualization; Maher Alharby: Conceptualization, methodology, validation, formal analysis, writing-review and editing, visualization; Ahmad Ali Hanandeh: Conceptualization, validation, formal analysis, writing-original draft preparation, writing-review and editing, visualization. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This research is supported by a grant (No. CRPG-25-3312) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

Conflict of interest

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

References

1. E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, M. Ilyas, Stacking ensemble deep learning for real-time intrusion detection in IoMT environments, *Sensors*, **25** (2025), 624. http://doi.org/10.3390/s25030624
2. M. Alharby, Blockchain-based system for secure storage and sharing of diabetics healthcare records, *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, Jeddah, Saudi Arabia, 2023, 1–6. http://doi.org/10.1109/ICAISC56366.2023.10085169
3. J. Areia, I. Bispo, L. Santos, R. L. D. C. Costa, IoMT-TrafficData: Dataset and tools for benchmarking intrusion detection in internet of medical things, *IEEE Access*, **12** (2024), 115370–115385. http://doi.org/10.1109/ACCESS.2024.3437214
4. J. A. Alzubi, O. A. Alzubi, I. Qiqieh, A. Singh, A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry, *IEEE T. Consum. Electr.*, **70** (2024), 2049–2057. http://doi.org/10.1109/TCE.2024.3350231
5. J. Ahmed, T. N. Nguyen, B. Ali, M. Javed, J. Mirza, On the physical layer security of federated learning based IoMT networks, *IEEE J. Biomed. Health*, **27** (2023), 691–697. http://doi.org/10.1109/JBHI.2022.3173947
6. A. Alamleh, O. S. Albahri, A. A. Zaidan, A. S. Albahri, A. H. Alamoodi, B. B. Zaidan, et al., Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems, *IEEE J. Biomed. Health*, **27** (2023), 878–887. http://doi.org/10.1109/JBHI.2022.3167256
7. J. Almalki, W. A. Shehri, R. Mehmood, K. Alsaif, S. M. Alshahrani, N. Jannah, et al., Enabling blockchain with IoMT devices for healthcare, *Information*, **13** (2022), 448. http://doi.org/10.3390/info13100448
8. M. S. Alkatheiri, A. S. Alghamdi, Blockchain-assisted cybersecurity for the internet of medical things in the healthcare industry, *Electronics*, **12** (2023), 1801. http://doi.org/10.3390/electronics12081801
9. S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, K. Saleem, BFT-IoMT: A blockchain-based trust mechanism to mitigate Sybil attack using fuzzy logic in the internet of medical things, *Sensors*, **23** (2023), 4265. http://doi.org/10.3390/s23094265

10. A. Barnawi, P. Chhikara, R. Tekchandani, N. Kumar, B. Alzahrani, A differentially privacy assisted federated learning scheme to preserve data privacy for IoMT applications, *IEEE Trans. Netw. Serv.*, **21** (2024), 4686–4700. http://doi.org/10.1109/TNSM.2024.3393969
11. B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, A. Kumar, Towards a secure and sustainable internet of medical things (IoMT): Requirements, design challenges, security techniques, and future trends, *Sustainability*, **15** (2023), 6177. http://doi.org/10.3390/su15076177
12. A. Berguiga, A. Harchay, A. Massaoudi, HIDS-IoMT: A deep learning-based intelligent intrusion detection system for the internet of medical things, *IEEE Access*, **13** (2025), 32863–32882. http://doi.org/10.1109/ACCESS.2025.3543127
13. P. Chandekar, M. Mehta, S. Chandan, Enhanced anomaly detection in IoMT networks using ensemble AI models on the CICIoMT2024 dataset, 2025, arXiv:2502.11854. http://doi.org/10.48550/arXiv.2502.11854
14. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, A. A. Ghorbani, CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT, *Internet Things*, **28** (2024), 101351. http://doi.org/10.1016/j.iot.2024.101351
15. K. Dhanushkodi, J. Shunmugiah, S. M. Velladurai, S. Rajendran, An optimal attention PLSTM-based classification model to enhance the performance of IoMT attack detection in healthcare application, *T. Emerg. Telecommun. T.*, **35** (2024), e5008. http://doi.org/10.1002/ett.5008
16. T. Daniya, M. Geetha, K. S. Kumar, Classification and regression trees with Gini index, *Advances in Mathematics Scientific Journal*, **9** (2020), 1857–8438. http://doi.org/10.37418/amsj.9.10.53
17. N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. K. M. Azad, S. A. Alyami, P. Liò, et al., SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization, *Electronics*, **12** (2023), 3541. http://doi.org/10.3390/electronics12173541
18. R. Guo, G. Yang, H. X. Shi, Y. H. Zhang, D. Zheng, O3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system, *IEEE Internet Things*, **8** (2021), 8949–8963. http://doi.org/10.1109/JIOT.2021.3055541
19. N. Garg, M. Wazid, J. Singh, D. P. Singh, A. K. Das, Security in IoMT-driven smart healthcare: A comprehensive review and open challenges, *Secur. Privacy*, **5** (2022), e235. http://doi.org/10.1002/spy2.235
20. A. Hafid, M. Rahouti, M. Aledhari, Optimizing intrusion detection in IoMT networks through interpretable and cost-aware machine learning, *Mathematics*, **13** (2025), 1574. http://doi.org/10.3390/math13101574
21. T. Hastie, S. Rosset, J. Zhu, H. Zou, Multi-class AdaBoost, *Stat. Interface*, **2** (2009), 349–360. http://doi.org/10.4310/SII.2009.v2.n3.a8
22. S. U. İlikhan, M. Özer, M. Perc, H. Tanberkan, Y. Ayhan, Complementary use of artificial intelligence in healthcare, *Medical Journal of Western Black Sea*, **9** (2024), 7–17. http://doi.org/10.29058/mjwbs.1620035
23. H. Jafarzadeh, M. Mahdianpari, E. Gill, F. Mohammadimanesh, S. Homayouni, Bagging and boosting ensemble classifiers for classification of multispectral, hyperspectral and PolSAR data: A comparative evaluation, *Remote Sens.*, **13** (2021), 4405. http://doi.org/10.3390/rs13214405

24. T. A. Khan, A. Fatima, T. Shahzad, A.-Ur-Rahman, K. Alissa, T. M. Ghazal, et al., Secure IoMT for disease prediction empowered with transfer learning in healthcare 5.0, the concept and case study, *IEEE Access*, **11** (2023), 39418–39430. http://doi.org/10.1109/ACCESS.2023.3266156
25. D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, Security in IoMT communications: A survey, *Sensors*, **20** (2020), 4828. http://doi.org/10.3390/s20174828
26. M. Kumar, Kavita, S. Verma, A. Kumar, M. F. Ijaz, D. B. Rawat, ANAF-IoMT: A novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC, *IEEE T. Ind. Inform.*, **18** (2022), 8936–8943. http://doi.org/10.1109/TII.2022.3181614
27. G. C. Lin, A. J. Lin, D. L. Gu, Using support vector regression and K-nearest neighbors for short-term traffic flow prediction based on maximal information coefficient, *Inform. Sciences*, **608** (2022), 517–531. http://doi.org/10.1016/j.ins.2022.06.090
28. J. K. Li, J. Castagna, Support vector machine (SVM) pattern recognition to AVO classification, *Geophys. Res. Lett.*, **31** (2004), L02609. http://doi.org/10.1029/2003GL018299
29. Q. Li, H. Q. Wei, D. L. Hua, J. L. Wang, J. X. Yang, Stabilization of semi-Markovian jumping uncertain complex-valued networks with time-varying delay: A sliding-mode control approach, *Neural Process. Lett.*, **56** (2024), 111. http://doi.org/10.1007/s11063-024-11585-1
30. A. Misbah, A. Sebbar, I. Hafidi, Securing internet of medical things: An advanced federated learning approach, *Int. J. Adv. Comput. Sc.*, **16** (2025), 1–12. http://doi.org/10.14569/IJACSA.2025.01602129
31. A. Misbah, A. Sebbar, I. Hafidi, Securing internet of medical things: An advanced federated learning approach, *Int. J. Adv. Comput. Sc.*, **16** (2025), 1–12. http://doi.org/10.14569/IJACSA.2025.01602129
32. I. D. Mienye, N. Jere, A survey of decision trees: Concepts, algorithms, and applications, *IEEE Access*, **12** (2024), 86716–86727. http://doi.org/10.1109/ACCESS.2024.3416838
33. S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, S. Verma, An intrusion detection mechanism for secured IoMT framework based on swarm-neural network, *IEEE J. Biomed. Health*, **26** (2022), 1969–1976. http://doi.org/10.1109/JBHI.2021.3101686
34. L. Nguyen, Tutorial on support vector machine, *Appl. Comput. Math.*, **6** (2016), 1–15. http://doi.org/10.11648/j.acm.s.2017060401.11
35. H. Naeem, A. Alsirhani, F. M. Alserhani, F. Ullah, O. Krejcar, Augmenting internet of medical things security: Deep ensemble integration and methodological fusion, *CMES-Comp. Model. Eng.*, **141** (2024), 2185–2223. http://doi.org/10.32604/cmes.2024.056308
36. G. R. Pradyumna, R. B. Hegde, K. B. Basavarajappa, T. Jan, G. R. Naik, Empowering healthcare with IoMT: Evolution, machine learning integration, security, and interoperability challenges, *IEEE Access*, **12** (2024), 20603–20623. http://doi.org/10.1109/ACCESS.2024.3362239
37. M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, et al., A survey on security threats and countermeasures in internet of medical things (IoMT), *T. Emerg. Telecommun. T.*, **33** (2020), e4049. http://doi.org/10.1002/ett.4049
38. A. Rácz, D. Bajusz, K. Héberger, Effect of dataset size and train/test split ratios in QSAR/QSPR multiclass classification, *Molecules*, **26** (2021), 1111. http://doi.org/10.3390/molecules26041111

39. A.-U. Rahman, M. U. Nasir, M. Gollapalli, S. A. Alsaif, A. S. Almadhor, S. Mehmood, et al., IoMT-based mitochondrial and multifactorial genetic inheritance disorder prediction using machine learning, *Comput. Intel. Neurosc.*, **2022** (2022), 2650742. http://doi.org/10.1155/2022/2650742
40. S. Razdan, S. Sharma, Internet of medical things (IoMT): Overview, emerging technologies, and case studies, *IETE Tech. Rev.*, **39** (2021), 775–788. http://doi.org/10.1080/02564602.2021.1927863
41. *Riskiest Devices 2025 Report*, 2025. Available from: `https://www.forescout.com/resources/riskiest-devices-2025-report/`.
42. M. Schonlau, R. Y. Zou, The random forest algorithm for statistical learning, *Stata J.*, **20** (2020), 3–29. http://doi.org/10.1177/1536867X20909688
43. P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, A. Gurtov, Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT, *IEEE J. Biomed. Health*, **27** (2023), 722–731. http://doi.org/10.1109/JBHI.2022.3186250
44. M. Santiago, H. Febiansyah, D. Dinarwati, Integrating machine learning with web intelligence for predictive search and recommendations, *International Transactions on Artificial Intelligence*, **3** (2024), 44–53. http://doi.org/10.33050/italic.v3i1.654
45. N. Syam, R. Kaul, Random forest, bagging, and boosting of decision trees, In: *Machine Learning and Artificial Intelligence in Marketing and Sales*, Leeds: Emerald Publishing, 2021, 139–182. http://doi.org/10.1108/978-1-80043-880-420211006
46. J. W. Tian, C. Shen, B. H. Wang, X. F. Xia, M. Zhang, C. H. Lin, et al., LESSON: Multi-label adversarial false data injection attack for deep learning locational detection, *IEEE T. Depend. Secure*, **21** (2024), 4418–4432. http://doi.org/10.1109/TDSC.2024.3353302
47. S. Umamaheswaran, J. M. Mannan, K. M. K. Raghunath, S. M. Dharmarajlu, M. D. Anuratha, RETRACTED: Smart intrusion detection system with balanced data in IoMT infra, *J. Intell. Fuzzy Syst.*, **46** (2024), 3191–3207.
48. A. J. Wyner, M. Olson, J. Bleich, D. Mease, Explaining the success of AdaBoost and random forests as interpolating classifiers, *J. Mach. Learn. Res.*, **18** (2017), 1–33.
49. M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, Y. Park, IoMT malware detection approaches: Analysis and research challenges, *IEEE Access*, **7** (2019), 182459–182476. http://doi.org/10.1109/ACCESS.2019.2960412
50. M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, J. J. P. C. Rodrigues, ASCP-IoMT: AI-enabled lightweight secure communication protocol for internet of medical things, *IEEE Access*, **10** (2022), 57990–58004. http://doi.org/10.1109/ACCESS.2022.3179418
51. S. Xu, Bayesian Naïve Bayes classifiers to text classification, *J. Inf. Sci.*, **44** (2018), 48–59. http://doi.org/10.1177/0165551516677946
52. W. C. Xing, Y. L. Bei, Medical health big data classification based on KNN classification algorithm, *IEEE Access*, **8** (2020), 28808–28819. http://doi.org/10.1109/ACCESS.2019.2955754
53. L. Yang, H. B. Wu, X. Q. Jin, P. P. Zheng, S. Y. Hu, X. L. Xu, et al., Study of cardiovascular disease prediction model based on random forest in eastern China, *Sci. Rep.*, **10** (2020), 5245. http://doi.org/10.1038/s41598-020-62133-5

54. L. Zhao, S. Lee, S.-P. Jeong, Decision tree application to classification problems with boosting algorithm, *Electronics*, **10** (2021), 1903. http://doi.org/10.3390/electronics10161903