Titre: Title:	Real-time anomaly detection in IoMT networks using stacking model and a healthcare-specific dataset
Auteurs: Authors:	Hadjer Goumidi, & Samuel Pierre
Date:	2025
Type:	Article de revue / Article
Référence: Citation:	Goumidi, H., & Pierre, S. (2025). Real-time anomaly detection in IoMT networks using stacking model and a healthcare-specific dataset. IEEE Access, 13, 70352-70365. https://doi.org/10.1109/access.2025.3563158

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 March 2025, accepted 14 April 2025, date of publication 21 April 2025, date of current version 29 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3563158

RESEARCH ARTICLE

Real-Time Anomaly Detection in IoMT Networks Using Stacking Model and a Healthcare-Specific Dataset

HADJER GOUMIDI AND SAMUEL PIERRE, (Senior Member, IEEE)
Mobile Computing and Networking Research Laboratory (LARIM), Department of Computer and Software Engineering, Polytechnique Montréal, Montreal, QC H3T 1J4, Canada

Corresponding author: Hadjer Goumidi (hadjer.goumidi@polymtl.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), in part by Prompt, in part by Flex Group, and in part by ISAME.

ABSTRACT The Internet of Medical Things (IoMT) connects medical devices to enable real-time monitoring and personalized care, significantly enhancing patient health and well-being. However, this connectivity also introduces substantial cybersecurity risks, including various attack types that compromise data integrity and availability, jeopardizing patient safety and healthcare service reliability. This study addresses these challenges by proposing a real-time anomaly detection model based on machine learning (ML) techniques, designed to detect and mitigate diverse cyber threats effectively. This paper proposes a new medical dataset for anomaly detection, inspired by the UNSW-NB15 dataset, and enriched with healthcare-relevant attack types, including falsification and DoS attacks, to reflect real-world IoMT scenarios. The dataset comprises 253 680 records, with 60% anomalous data distributed across multiple attack types, offering a more challenging and realistic environment for evaluating ML models. Seven machine learning algorithms, including Random Forest, XGBoost, and Artificial Neural Networks (ANN), were rigorously tested, leading to the development of a novel stacking ensemble model. This model integrates XGBoost as the meta-learner with Random Forest and ANN as base models, leveraging their strengths to optimize anomaly detection. The proposed model was evaluated on both the UNSW-NB15 and the new medical dataset, achieving significant improvements across key metrics such as accuracy, precision, recall, and F1-score. A real-time prediction analysis further demonstrated its ability to detect anomalies efficiently during live data transmission, validating its suitability for detecting anomalies in real-time scenarios.

INDEX TERMS Anomaly detection, intrusion detection system, Internet of Medical Things, medical dataset with anomalies, machine learning, healthcare security.

I. INTRODUCTION

The Internet of Medical Things (IoMT) has revolutionized modern healthcare by seamlessly connecting medical devices, wearable sensors, and healthcare IT systems [1]. This interconnected ecosystem enables real-time patient monitoring, personalized treatment plans, and efficient care delivery, significantly enhancing healthcare quality and patient outcomes. Devices such as smart infusion pumps, wearable health monitors and connected diagnostic tools empower healthcare providers to make timely interventions and deliver tailored care strategies. Beyond clinical benefits, IoMT reduces costs, improves operational efficiency, and increases accessibility to medical services, holding immense potential to redefine healthcare systems globally [1], [2].

However, the integration of IoMT devices into healthcare networks introduces significant cybersecurity challenges. These devices often operate with limited computational resources and lack robust security features, making them vulnerable to cyberattacks such as data falsification, denial of service (DoS) attacks, and message tampering [3], [4]. Such threats can compromise the integrity and availability

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

of critical healthcare systems, with severe consequences. For instance, a falsified message from an insulin pump could lead to incorrect dosages, or a DoS attack could disrupt vital monitoring systems during emergencies, endangering patient lives [5].

Traditional security measures, including cryptographic techniques like hashing and encryption, are essential but often impose computational demands that exceed the capabilities of resource-constrained IoMT devices [5], [6]. For example, ensuring message integrity through hashing can be computationally expensive for medical devices. Moreover, even encrypted data remains vulnerable to integrity and availability threats. To address these limitations, machine learning (ML)-based anomaly detection systems have emerged as a promising solution, enabling real-time analysis of incoming data to identify tampering, disruptions, or malicious activity.

To support this effort, we developed a new medical dataset for anomaly detection that reflects real-world healthcare scenarios and addresses the limitations of existing datasets. By incorporating features and attacks inspired by the UNSW-NB15 dataset [7] and introducing attacks that significantly impact healthcare systems, such as falsification and DoS attacks, this dataset provides a comprehensive foundation for evaluating Intrusion Detection Systems (IDS) solutions. It includes diverse normal and anomalous data, balancing complexity and practicality for IoMT security research. Using this dataset, we evaluated seven ML algorithms, XGBoost [31], Random Forest [30], ANN [32], Support Vector Machines (SVM) [28], K-Nearest Neighbors (KNN) [27], Logistic Regression (LR) [29], and Isolation Forest (IF) [29], and selected XGBoost, Random Forest, and ANN as base learners for their strong accuracy and efficiency. These algorithms were integrated into a novel stacking ensemble model, with XGBoost serving as the meta-learner, to achieve robust and efficient anomaly detection tailored to IoMT environments.

This research addresses the cybersecurity challenges of IoMT, particularly data integrity and availability, through a real-time anomaly prediction model. The model dynamically adapts to incoming messages and newly detected anomalies or attack types. To overcome the lack of specialized datasets for healthcare systems, we developed a new medical dataset combining medical data with IoT network attacks (e.g., Fuzzers, Shellcode, Worms, Exploit) and healthcare-relevant attacks (e.g., Data Falsification and DoS). Additionally, we proposed a stacking ensemble model that demonstrates superior accuracy and efficiency, offering a reliable solution for real-time anomaly detection in healthcare environments.

To guide this research work, the study is driven by the following research questions:

1. How can a synthetic medical dataset that integrates healthcare data with diverse network attack types improve the development and evaluation of anomaly detection models for IoMT?
2. Which machine learning algorithms are most suitable for detecting and classifying both generic and healthcare-specific attacks (such as data falsification and DoS) with high accuracy and reliability?
3. Can a stacking ensemble model enhance the detection performance across multiple attack categories?
4. How effective is the proposed model in performing real-time anomaly prediction during live data transmission, and what levels of accuracy can be achieved in such a setting?

The key contributions of this research are as follows:

1) We proposed a real-time anomaly detection model based on machine learning, capable of pre-training datasets and dynamically predicting attacks in real time.
2) We developed a new medical dataset for anomaly detection that integrates medical data with known IoT network attacks inspired by UNSW-NB15 dataset and healthcare-relevant attack types such as falsification and DoS attacks to address real-world IoMT challenges.
3) We evaluated the performance of seven machine learning algorithms across both the UNSW-NB15 and the new medical datasets to identify the most effective models for anomaly detection.
4) Based on the evaluation results, we designed a novel stacking ensemble model that integrates the best-performing algorithms to enhance anomaly detection and real-time prediction capabilities.
5) We conducted a real-time prediction analysis by sending 100 sequential messages containing normal and anomalous data and performed real-time anomaly detection during live data transmission.
6) Our proposed stacking model demonstrated superior performance, significantly improving accuracy and efficiency, and demonstrating reliable performance across diverse attack types.

The originality of this paper lies in developing a real-time anomaly detection model that dynamically detects anomalies during live data transmission, creating a medical dataset enriched with real-world attack types, and proposing a high-performing stacking model with superior accuracy and efficiency for real-time IoMT applications.

This paper is organized as follows. Section II provides an overview of related works, focusing on machine learning methods and anomaly detection systems for IoT networks and IoMT. Section III explains the methodology, describing the proposed anomaly detection model and stacking algorithm. Section IV discusses experiments, including the feature selection and the creation of the new dataset, as well as presenting the results including the performance of ML models and the proposed stacking algorithm on both datasets and the real-time prediction analysis. Finally, Section V concludes the paper and suggests future directions for improving anomaly detection systems in IoMT environments.

II. RELATED WORK

The increasing use of machine learning for anomaly detection in IoMT and IoT networks has led to diverse approaches, datasets, and methodologies. This section reviews key contributions, focusing on anomaly detection techniques, ensemble frameworks, and their applications in healthcare and IoT security. A comparison of prior works is provided in Appendix.

In [8], five machine learning algorithms were evaluated on the MIT-BIH dataset for heart rate anomaly detection. While effective, the study defined variables outside the fixed range (60–100 bpm) as anomalies, which limited its real-world applicability. Local Outlier Factor (LOF) and Random Forest performed best, highlighting the potential of simulated data for training. Park et al. [9] used GANs to generate fraud labels for datasets lacking them, applying logistic regression and XGBoost for classification, with SHAP analysis identifying key features. In [10], unsupervised clustering (K-means and K-medoids) was used to detect anomalies in wearable sensor data, with K-means slightly outperforming K-medoids. However, dataset details were lacking. In [11], the DIB system used R-FCVM (rough set theory and fuzzy core vector machine) to detect illegal device behavior in medical IoT but did not address data anomalies. Alsolami et al. [12] explored ensemble learning (Bagging, Boosting, Stacking) for IoMT anomaly detection using the WUSTL-EHMS-2020 dataset [13], though its small size and limited attack types hindered comprehensive evaluation. In IoT, Ullah and Mahmoud [14] used CNNs for multiclass anomaly detection, achieving high accuracy with BoT-IoT and IoT-23 datasets. Das et al. [15] introduced a hybrid ensemble method for detecting known and zero-day DDoS attacks, achieving 99.1% accuracy on NSL-KDD and UNSW-NB15 datasets. Gu et al. [16] proposed a semi-supervised k-means algorithm for DDoS classification, though it lacked accuracy benchmarks. Meidan et al. [17] developed N-BaIoT using deep autoencoders for IoT devices, effective but without accuracy metrics. Ravi and Shalinie [18] proposed a semi-supervised deep extreme learning machine (SDELM) for DDoS mitigation, though limited to UDP flooding attacks on the UNB-ISCX dataset. Doshi et al. [19] presented a four-stage anomaly detection pipeline with high accuracy but relied on synthetic data. Maseer et al. [20] evaluated 31 ML models, identifying k-NN, Decision Trees, and Naive Bayes as top performers on CICIDS2017.

Other works addressed domain-specific challenges. Choi et al. [21] compared deep anomaly detection models for time-series data. Luo et al. [22] used stacked autoencoders (SAE) for early fault detection in CNC machines. Abdelmoumin et al. [23] explored PCA and one-class SVM for scalable IDS development. Poornima and Paramasivan [24] proposed a regression-based approach to reduce computational complexity in Wireless Sensor Networks. Kavitha et al. [10] used logistic regression and ANN for IoT anomaly detection, with ANN outperforming logistic regression on DS2OS. Alsamiri and Alsubhi [25] evaluated seven ML algorithms on Bot-IoT, improving detection with new features. Hasan et al. [26] integrated XAI with ensemble classifiers for Bitcoin anomaly detection, proposing XGB-CLUS for data balancing, which outperformed traditional methods.

Existing literature highlights limitations, such as the lack of comprehensive medical datasets and real-time intrusion detection evaluation. While ensemble methods like voting and stacking have been explored, their real-time application in IoMT remains underdeveloped. To address these gaps, this research introduces a new medical anomaly detection dataset combining medical data with UNSW-NB15-inspired attacks, enriched with healthcare-relevant threats. A novel stacking ensemble model (XGBoost, Random Forest, ANN) is proposed. The evaluation of the proposed model is performed in real-time scenarios, demonstrating robustness and efficiency in practical healthcare settings.

III. METHODOLOGY

This section presents the proposed real-time anomaly detection model and the stacking ensemble model, along with the machine learning (ML) algorithms analyzed in this work.

A. THE PROPOSED REAL-TIME ANOMALY DETECTION MODEL

Healthcare systems operate in dynamic environments where vast amounts of data are continuously generated and transmitted by connected devices. Real-time anomaly detection is critical in this context, as delays in identifying malicious activity can lead to severe consequences, including unauthorized access, falsification of patient data, and disruption of healthcare services. To enhance healthcare system security, we propose a real-time anomaly detection model, as illustrated in Fig. 1. The model consists of two primary components: Medical Devices and Edge Computing.

1) MEDICAL DEVICES

This component represents the data collection process involving devices, such as wearables and medical sensors. We assume the collected data is encrypted using a lightweight and efficient encryption algorithm to ensure confidentiality. However, during transmission to the edge layer, attacks may compromise the integrity and availability of the ciphertext.

2) EDGE COMPUTING

This component plays a crucial role in data analysis and system security. In this paper, the edge computing layer was simulated using a local machine (PC), which acted as a lightweight edge node responsible for both model pretraining and real-time data stream processing. It operates in two main phases:

- Pretraining Phase: Before deployment, the model is trained on the new medical dataset, which includes both normal and anomalous data. This phase enables the

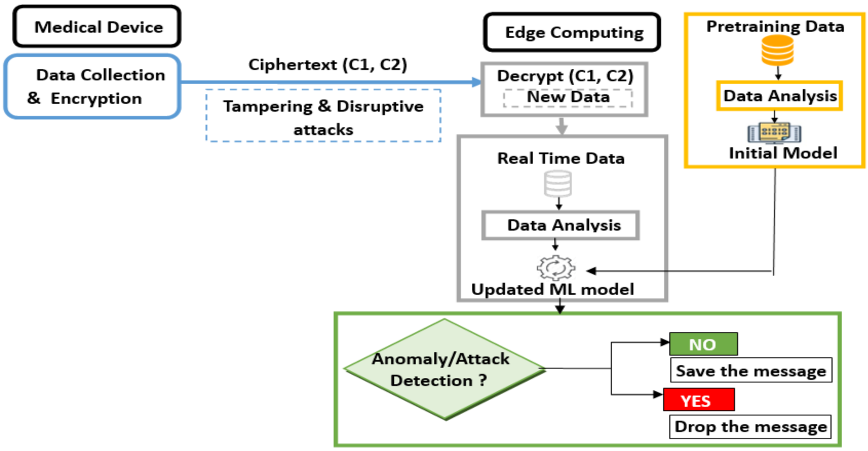


FIGURE 1. The proposed real-time anomaly prediction model.

model to understand typical network behavior and detect unusual activity.

- Real-Time Data Processing Phase: Once deployed, the model dynamically processes incoming data streams in real-time. Each data point is analyzed immediately after decryption, allowing instant classification as normal or anomalous. This capability ensures timely identification and response to potential threats.

The model continuously adapts by learning from new patterns, enhancing its ability to detect and predict previously unseen anomalies. This ensures robust network monitoring, enabling the system to identify and mitigate emerging threats, thereby maintaining healthcare system security and integrity.

B. THE PROPOSED STACKING-ENSEMBLE LEARNING MODEL

Based on the literature review, seven ML algorithms were selected. These models were analyzed to identify the best performers and integrated into a stacking-based ensemble learning model to enhance real-time prediction accuracy and efficiency.

1) ML SELECTED ALGORITHMS

To evaluate the performance of diverse learning strategies in anomaly detection, we selected seven machine learning models widely adopted in the literature for their effectiveness in classifying and predicting anomalies.

- K-Nearest Neighbors (KNN): A simple, effective method for pattern detection, chosen for its ability to classify data based on proximity [27].
- Support Vector Machine (SVM): A robust classifier for high-dimensional data, selected for its effectiveness in separating complex patterns [28].
- Logistic Regression (LR): A straightforward binary classifier, preferred for its simplicity and interpretability in distinguishing anomalies [29].
- Random Forest: An ensemble model that reduces overfitting, chosen for its accuracy and reliability in classification tasks [30].
- Isolation Forest (IF): An unsupervised algorithm ideal for anomaly detection, selected for its efficiency with high-dimensional data [29].
- XGBoost: A high-performance gradient boosting method, chosen for its ability to handle large datasets and complex tasks [31].
- ANN: A powerful model for non-linear data, selected for its capability to detect intricate attack patterns [32].

2) STACKING- ENSEMBLE LEARNING

Our proposed ensemble model uses a stacking-based methodology [33] to improve intrusion detection system performance by leveraging the strengths of multiple ML algorithms. The model integrates three base learners, XGBoost, Random Forest, and ANN, with XGBoost serving as the meta-learner to refine and optimize final predictions. Fig. 2 illustrates the stacking ensemble framework.

The base learners were selected based on their demonstrated effectiveness during evaluation (see Section IV-C). XGBoost excels at modeling non-linear relationships and addressing misclassifications through iterative refinement. Random Forest enhances robustness with its bagging-based approach, reducing variance and ensuring stability. ANN complements these models by capturing intricate, non-linear patterns, improving the ensemble's ability to differentiate between normal traffic and various attack types. These algorithms consistently delivered high accuracy, precision, recall, and F1-scores, along with strong AUC values.

They also exhibited faster testing times compared to other algorithms like SVM and KNN, which, despite acceptable performance, were computationally expensive for real-time detection.

In the stacking framework, the outputs from the base learners are passed to the meta-learner (XGBoost), which combines their predictions to produce the final classification.

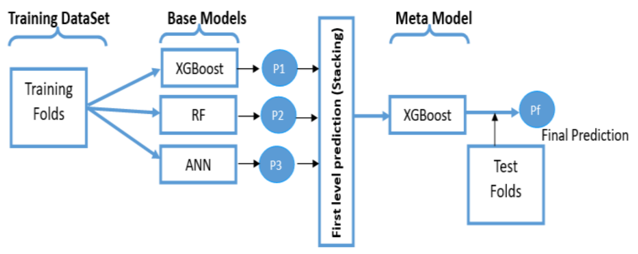


FIGURE 2. **Stacking ensemble learning algorithm.**

Each base learner is independently trained, and its predictions are used as input features for the meta-model. This architecture enables the meta-learner to mitigate individual model weaknesses and leverage their combined strengths for more accurate predictions, as detailed in Algorithm 1.

By integrating the strengths of XGBoost, Random Forest, and ANN, the proposed stacking ensemble model provides a reliable and efficient solution for anomaly detection, capable of detecting a wide range of attacks while remaining suitable for real-time deployment.

Algorithm 1 Ensemble Stacking Model With Multiple Base Models and K-Fold Cross-Validation

Input: Dataset features X, numerical and categorical features from the UNSW-NB15 dataset/Medical dataset with attacks.
Target variable y: attack labels indicating normal or various attack types.
Step 1: Select a K-fold split of the dataset.
Step 2: Select M base models.
Base Models: Define $M = \{M_1, M_2, M_3\}$
M_1: XGBoost;
M_2: Random Forest;
M_3: Artificial Neural Network (ANN).
Step 3: Train Base Models:
For each base model $M_i \in M$:
Evaluate using K-Fold Cross-Validation.
Store the out-of-fold predictions for each instance.
Train M_i on the full training set (X_{train}, y_{train}) for final use.
Step 4: Train meta-learner:
Combine the out-of-fold predictions from all base models into a new feature matrix $P=\{P_1, P_2, P_3\}$, where:
P_1, P_2, P_3 are predicted from M_1, M_2, M_3 respectively.
Step 5: Train the meta-learner (XGBoost) using the combined feature matrix P and the corresponding attack labels y_{train}.
Output: The evaluation metrics & the predicted attack classes ($\hat{y}$) for each instance in real-time data.

IV. EXPERIMENTS

This section outlines the data analysis process, as depicted in Fig. 3. It begins with a description of the datasets used, followed by data pre-processing steps, attack generation methods, and evaluation metrics for assessing the performance of the machine learning (ML) algorithms and the proposed stacking model. Finally, the results are presented and discussed.

The experiments were conducted on a system with an Intel(R) Core(TM) i7-8650U CPU @ 1.90 GHz, 16 GB of RAM, and Windows 10 (64-bit). All tasks, including model implementation and feature engineering, were performed using Python 3 within the Anaconda environment. Data transmission was simulated using an Arduino, representing the medical device, while the edge computing component was executed on the machine running the Python code.

To ensure optimal model performance, hyperparameters were meticulously selected and fine-tuned, as detailed in Table 1.

A. DATASETS DESCRIPTION

In this paper. we have used two public datasets: The UNSW-NB15 dataset [7] and the Behavioral Risk Factor Surveillance System (BRFSS) dataset for 2015 [34]. In this section. we describe both datasets and their pre-processing phase.

1) UNSW-NB15 DATASET

The UNSW-NB15 dataset [7], introduced by the Australian Centre for Cyber Security (ACCS), provides a modern representation of synthetic network traffic, including normal and abnormal activities. It contains 2.5 million records, with one normal class and nine attack categories: Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, and Worms. The dataset is organized into six feature groups (flow, basic, content, time, additional generated, and labeled features), comprising 49 features in total [7].

For this study, a 10% cleaned subset of the UNSW-NB15 dataset, consisting of 175,341 training records and 82,332 test records, was used. The dataset includes 47 features with numeric, nominal, and categorical data types labeled for both binary and multi-class classification. Fig. 4 depicts the distribution of each attack type in the training and testing sets.

2) MEDICAL DATASET

Publicly available medical datasets incorporating anomalies and simulated attacks are scarce. While some datasets, such as heart rate monitors, exist, they are limited in scope and lack comprehensive medical data or diverse attack types. The WUSTL-EHMS-2020 dataset [13], containing approximately 16,000 records, includes IoMT-specific attacks but is small and lacks diversity in attack scenarios.

To address these limitations, we modified the BRFSS dataset for 2015, which contains physiological medical data. The BRFSS [34] is an annual health survey conducted by the CDC, collecting responses from over 400,000 Americans on health behaviors, chronic conditions, and preventive services. It includes 253,680 records and 22 features representing

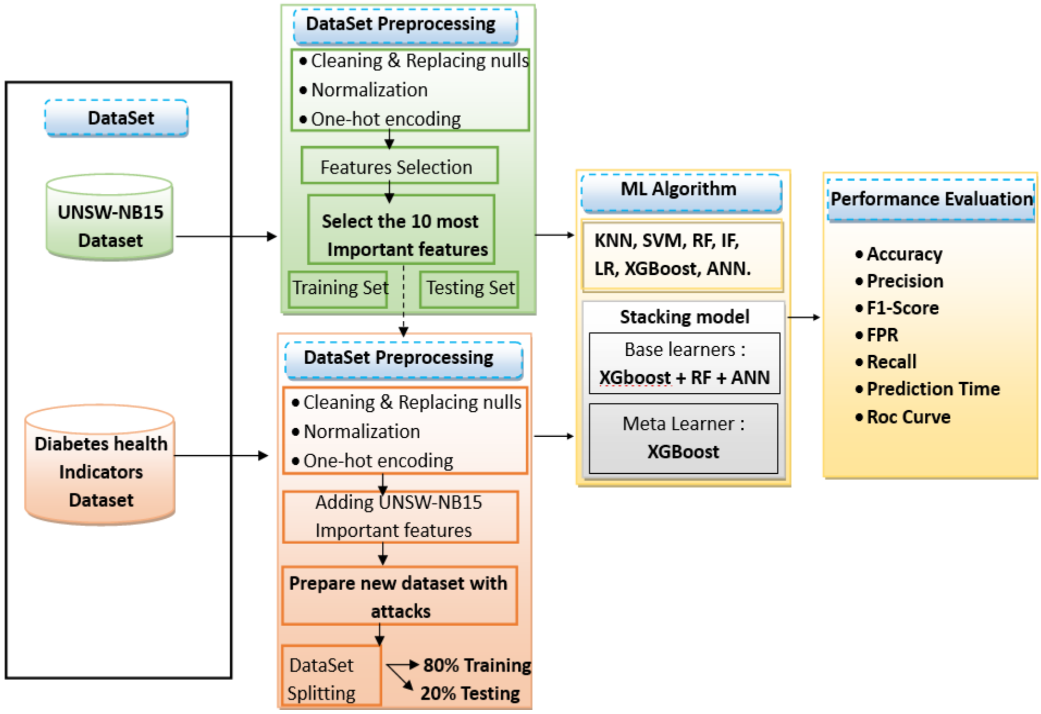


FIGURE 3. The workflow of the proposed methodology for anomaly detection in IoMT.

TABLE 1. The hyperparameter values of the analysed ML models.

Model	Hyperparametres
XGBoost	n_estimators=500, learning_rate=0.01, max_depth=5, min_samples_split=8, min_samples_leaf=4, subsample=0.8, random_state=42
RF	n_estimators=200, max_depth=15, min_samples_split=10, min_samples_leaf=5, max_features='sqrt', random_state=42
LR	random_state=42, max_iter=1000, solver='saga', penalty='l2', C=1.0
ISOF	contamination=0.6, random_state=42
KNN	n_neighbors=3, weights='distance', metric='minkowski'
ANN	hidden_layer_sizes=(100, 50, 20), max_iter=1000, random_state=42, learning_rate_init=0.001, activation='relu'
SVM	kernel='rbf', probability=True, random_state=42, C=5.0, gamma='scale'
Stacking model	(n_estimators=100, max_depth=5, learning_rate=0.01, random_state=42), cv=5

various health indicators, such as lifestyle choices, physical conditions, and medical history.

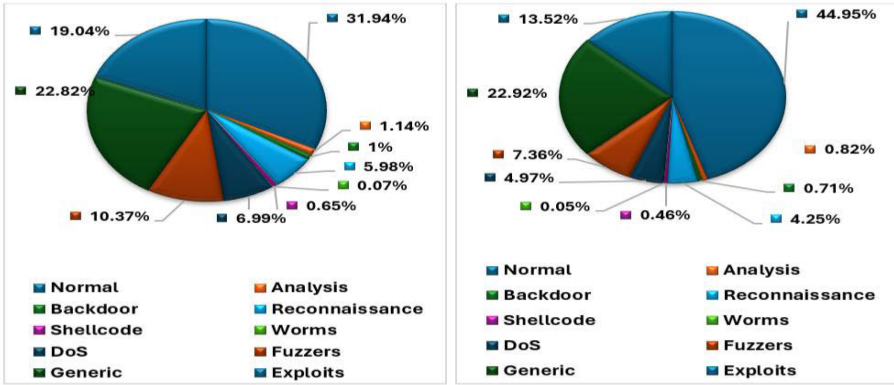
3) DATA PRE-PROCESSING

Data pre-processing is crucial to ensure clean, consistent, and suitable datasets for anomaly and attack detection. This phase involved cleaning, transforming, and organizing the data to improve its quality and compatibility with ML algorithms.

- Handling Missing and Invalid Values: Missing or invalid values were replaced with appropriate substitutes to preserve data integrity.
- Encoding Categorical Features: Categorical features were converted into numerical representations using ordinal encoding and one-hot encoding.
  Ordinal encoding assigned unique integer values to each category, while one-hot encoding created binary vectors to represent distinct categories without introducing unintended ordinal relationships.
- Data Normalization: Normalization was applied to scale features, particularly for algorithms like SVM, LR, ANN, and KNN, which are sensitive to input feature scales. Min-Max Scaling was used to rescale features to a range of 0 to 1 using the formula:

$$X_{new} = \frac{X_i - X_{min}}{(X_{max} - X_{min})}, \tag{1}$$

  where X_i is the original feature value; and X_{min} and X_{max} are the minimum and maximum values of the feature, respectively.
- Feature Selection: XGBoost was employed for feature selection on the UNSW-NB15 dataset due to its ability to handle numerical and categorical features while capturing complex, non-linear patterns. Feature importance scores were calculated to identify and retain the most impactful features, reducing dimensionality and improving model efficiency. For the medical dataset, all 22 physiological features were retained, as any could be targeted by attacks like falsification.



(a) (b)

FIGURE 4. **Data Distribution by normal and attack types in the UNSW-NB15 dataset: (a) Training set and (b) Testing set.**

- To address the significant class imbalance observed across different attack types, we applied the Synthetic Minority Over-Sampling Technique (SMOTE) to the training set. This approach was used to artificially generate new samples for under-represented classes, helping to improve the learning capacity of the model, especially for minority attack categories such as Worms and Shellcode.

B. THE NEW MEDICAL DATASET WITH ATTACKS

The new medical dataset for anomaly detection was created by drawing inspiration from the UNSW-NB15 dataset. Attack scenarios were generated and incorporated into the dataset to simulate real-world threats, ensuring a comprehensive foundation for evaluating intrusion detection systems.

1) UNSW-NB15 ATTACKS INSPIRATION

The original goal of the BRFSS (Behavioral Risk Factor Surveillance System) dataset is diabetes prediction, in this paper, we restructured it to simulate cybersecurity attack scenarios within healthcare data. Guided by the UNSW-NB15 dataset, we evaluated attack types for relevance to our case study, as illustrated in Table 2.

Attacks like Backdoor, Analysis, Generic, and Reconnaissance, which primarily impact data confidentiality, were excluded as they fall outside our scope. We retained normal data and attack types affecting data integrity and availability, which are critical in healthcare settings. To enhance the BRFSS dataset, we integrated the 10 most relevant features from UNSW-NB15 (illustrated in Fig. 5) and introduced new features for simulating network attacks. Normal data was used as a baseline, with features systematically modified to simulate attacks inspired by UNSW-NB15.

2) ATTACKS GENERATION

To improve dataset realism, we focused on two critical healthcare threats: falsification attacks and Denial of Service (DoS) attacks. Falsification attacks compromise data integrity by altering or injecting false information, while DoS attacks disrupt service availability by overwhelming network resources.

TABLE 2. **Attacks type description in UNSW-NB15 dataset.**

Attack Type	**Description**	**Affected Services**
DoS	Overloads network services	**Availability**
Backdoor	Gains illegal system access	Confidentiality, integrity
Analysis	Probes for application vulnerabilities	Confidentiality
Exploits	Exploits network vulnerabilities	**Integrity, Confidentiality**
Fuzzers	Tests for system weaknesses	**Integrity, Availability**
Generic	Breaks cryptographic systems	Confidentiality, integrity
Reconnaissance	Gathers network information	Confidentiality
Shellcode	Executes malicious code	**Integrity**
Worms	Spreads self-replicating malware	**Availability, Integrity**

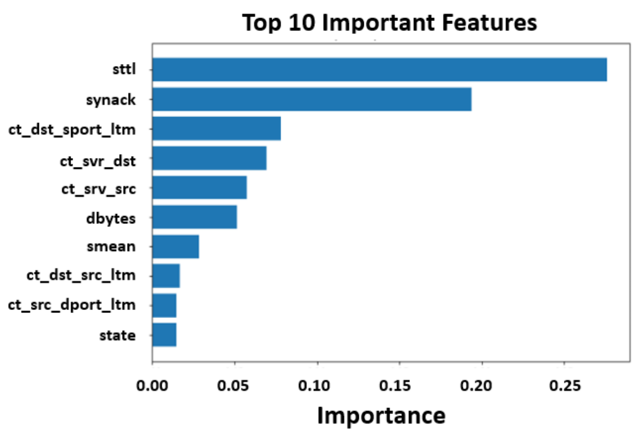


FIGURE 5. **The most ten important features on the UNSW-NB15 dataset.**

Since UNSW-NB15 lacks falsification attacks and has limited DoS samples, we enriched our dataset with realistic instances of these attacks.

A real-world-inspired scenario was designed, simulating data transmission from an Arduino (i.e., medical device) to a laptop (i.e., edge computing system). For falsification attacks, Ettercap was used to intercept and modify encrypted medical data during transmission, simulating tampering with sensitive information. For DoS attacks, HPING3 generated high-volume traffic floods (e.g., ICMP, TCP SYN, UDP floods, etc.), overwhelming network resources and disrupting communication. These additions provide critical examples of data integrity breaches and resource-based disruptions, enhancing the dataset's ability to reflect real-world medical network threats.

3) NEW MEDICAL DATASET FOR ANOMALY DETECTION

The new medical dataset integrates patient health data with network anomaly features and simulated attack scenarios, offering a comprehensive resource for evaluating anomaly detection systems in healthcare. It contains 253,680 rows, each representing normal activity or an attack, with 32 features blending medical and network-related attributes.

- Medical Features: 22 indicators (e.g., cholesterol, blood pressure, BMI) from the original BRFSS dataset, retained to reflect real-world healthcare scenarios.
- Network Features: 10 relevant features from UNSW-NB15 (see Fig. 5), were selected for their importance in predicting attacks that harm data integrity and availability.

The dataset includes six attack types alongside normal traffic; Normal activity accounts for 40% of the dataset, while the remaining 60% comprises various attacks: Falsification attacks (20.3%), which represent data integrity breaches by manipulating encrypted medical information during transmission; Denial of Service (DoS) attacks (15%), which simulate resource exhaustion and communication disruptions; Fuzzers (11%), which inject random data to exploit vulnerabilities; Exploits (12%), targeting system weaknesses for unauthorized access; Worms (1%), representing self-replicating malware; and Shellcode (1%), involving malicious code execution. Attack distributions were inspired by UNSW-NB15, with adjustments to emphasize critical healthcare threats like falsification and DoS.

This dataset provides a unique combination of medical data and network anomaly scenarios, offering a valuable resource for developing robust anomaly detection systems tailored to secure healthcare networks against real-world threats.

4) EVALUATION METRICS

The evaluation metrics for the machine learning models were derived from the confusion matrix, as detailed in Table 3. The confusion matrix organizes the four possible classification outcomes in a binary classifier: True Positive (TP), where the model correctly identifies attacks; True Negative (TN), where it correctly classifies benign data; False Positive (FP), where benign data is incorrectly classified as an attack; and False Negative (FN), where an attack is incorrectly classified as benign, potentially leading to undetected threats. In this study, several standard evaluation metrics were used to assess model performance, as outlined in Table 4. Additionally, training and testing times were measured for each model to evaluate computational efficiency, which is critical for real-time anomaly detection in healthcare applications where rapid decision-making is essential.

In this paper, reliability refers to the consistency and robustness of a model's performance across a wide range of attack categories and scenarios. Efficiency refers to the model's ability to process and classify data quickly, which is especially important for real-time anomaly detection.

TABLE 3. Confusion matrix.

	Predicted Normal	Predicted Attack
Attack actual	FN	TP
Normal actual	TN	FP

TABLE 4. Evaluation metrics for model performance.

Metric	Description	Formula
Accuracy	Measures overall correctness.	$\frac{(TP+TN)}{Total}$
Precision	Identifies true attacks precisely.	$\frac{TP}{(FP+TP)}$
False Positive Rate (FPR)	Tracks misclassified normal instances.	$\frac{FP}{(FP+TP)}$
Recall	Captures all true attacks.	$\frac{TP}{(FN+TP)}$
F1 score	Balances precision and recall.	$\frac{2*(Precision*Recall)}{(Precision+Recall)}$
ROC-AUC Score	Assesses model's separability.	

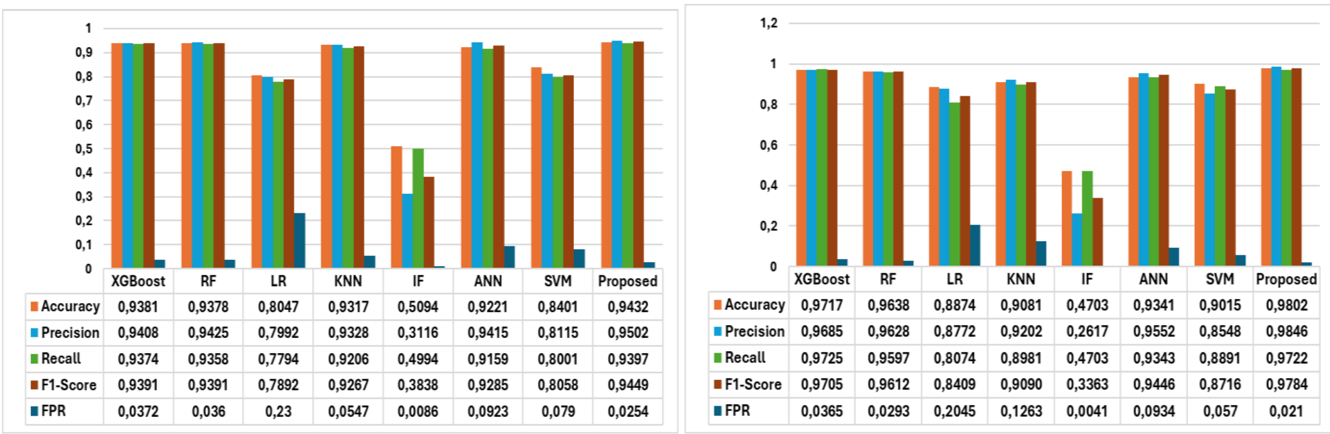
C. PERFORMANCE EVALUATION AND DISCUSSION

The performance evaluation was conducted in two phases: the pretraining phase and the real-time prediction phase.

1) PRETRAINING PHASE

During the pretraining phase, models were trained and validated on the UNSW-NB15 dataset and a new medical dataset for anomaly detection, as shown in Fig.6 (a) and (b), respectively. The results revealed significant improvements in model performance on the medical dataset compared to UNSW-NB15. XGBoost achieved the highest accuracy, improving from 93.81% on UNSW-NB15 to 97.17% on the medical dataset. Random Forest and ANN also showed notable improvements, with their accuracy increasing from 93.78% to 96.38% and from 92.21% to 93.41%, respectively. These results validated the selection of XGBoost, Random Forest, and ANN as base models for the proposed stacking model, with XGBoost serving as the meta-learner.

The stacking model outperformed all other models, achieving 98.02% accuracy on the medical dataset compared to



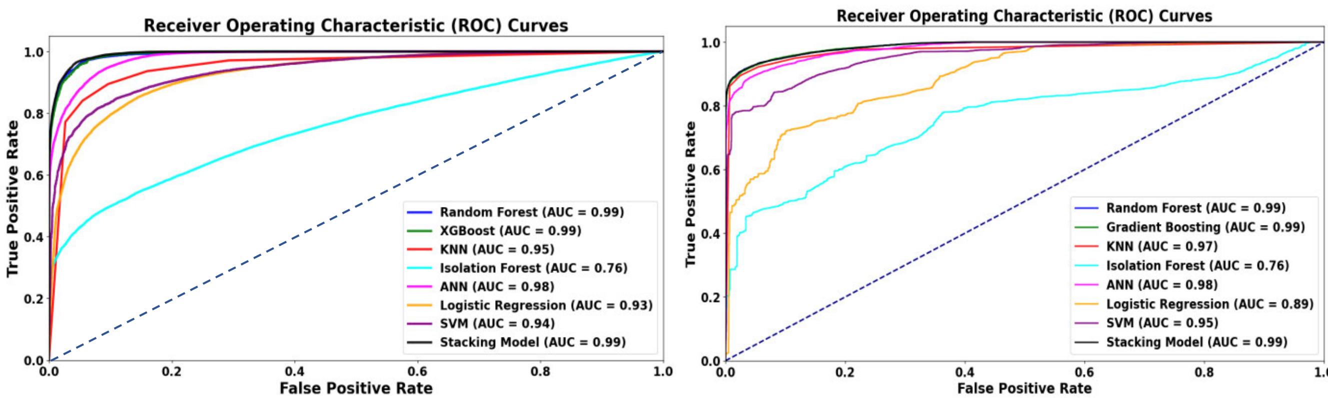
	XGBoost	RF	LR	KNN	IF	ANN	SVM	Proposed
Accuracy	0,9381	0,9378	0,8047	0,9317	0,5094	0,9221	0,8401	0,9432
Precision	0,9408	0,9425	0,7992	0,9328	0,3116	0,9415	0,8115	0,9502
Recall	0,9374	0,9358	0,7794	0,9206	0,4994	0,9159	0,8001	0,9397
F1-Score	0,9391	0,9391	0,7892	0,9267	0,3838	0,9285	0,8058	0,9449
FPR	0,0372	0,036	0,23	0,0547	0,0086	0,0923	0,079	0,0254

(a)

	XGBoost	RF	LR	KNN	IF	ANN	SVM	Proposed
Accuracy	0,9717	0,9638	0,8874	0,9081	0,4703	0,9341	0,9015	0,9802
Precision	0,9685	0,9628	0,8772	0,9202	0,2617	0,9552	0,8548	0,9846
Recall	0,9725	0,9597	0,8074	0,8981	0,4703	0,9343	0,8891	0,9722
F1-Score	0,9705	0,9612	0,8409	0,9090	0,3363	0,9446	0,8716	0,9784
FPR	0,0365	0,0293	0,2045	0,1263	0,0041	0,0934	0,057	0,021

(b)

FIGURE 6. **Performance analysis of the ML anomaly prediction models running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomalyprediction.**



(a) (b)

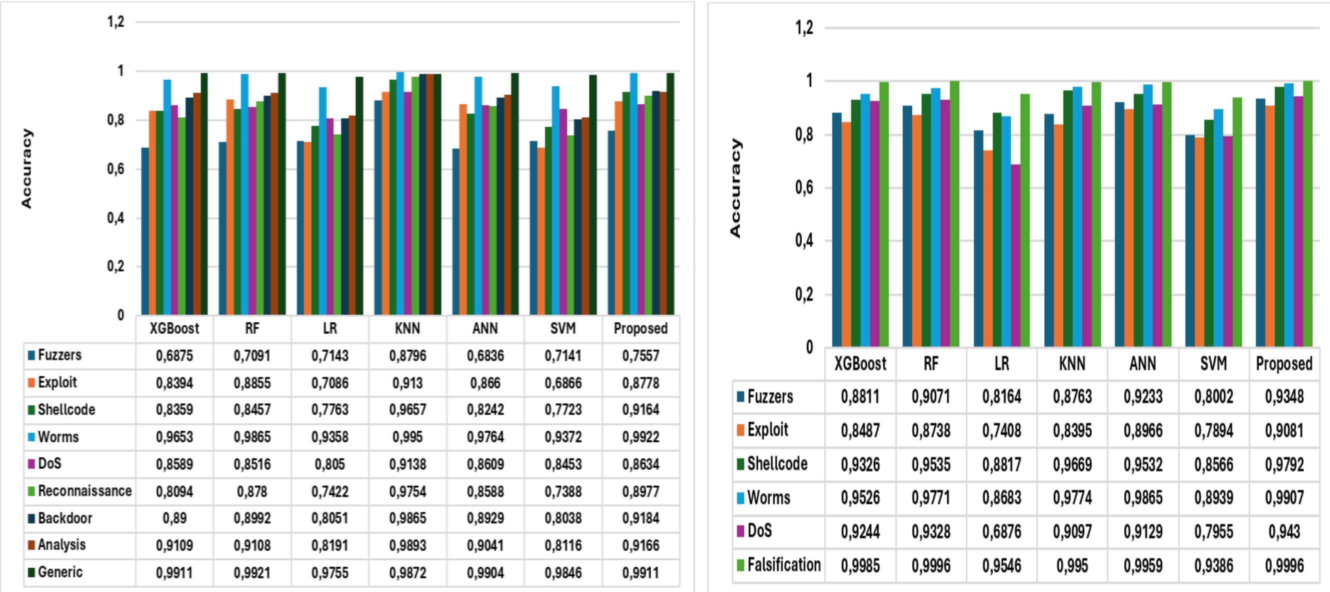
FIGURE 7. **Roc Curve of the ML anomaly prediction models running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomaly prediction.**

94.32% on UNSW-NB15. SVM and Logistic Regression showed moderate improvements, while KNN experienced a slight decline in performance due to the inclusion of falsification attacks, which disrupted proximity-based relationships. Isolation Forest consistently performed poorly, reflecting its unsupervised nature and inability to effectively capture structured patterns in the datasets.

To further evaluate model performance, ROC curves and AUC values were analyzed (see Fig. 7). XGBoost, Random Forest, and ANN achieved AUCs of 0.99, 0.99, and 0.98, respectively, on both datasets, confirming their ability to rank anomalies accurately and handle complex features. The stacking model achieved an AUC of 0.99, leveraging the complementary strengths of its base models for enhanced anomaly detection. In contrast, models like KNN, SVM, and Logistic Regression exhibited slightly lower AUC values, while Isolation Forest recorded the lowest AUC of 0.76, reflecting its limited ability to handle structured datasets.

The evaluation of model accuracy for predicting specific attack types across the two datasets highlighted the strengths of the proposed stacking model, as displayed in Fig. 8. It consistently achieved high accuracy across all attack types, particularly on the new medical dataset, where it excelled in detecting the falsification attack. KNN also demonstrated strong accuracy in identifying various attacks, though its high testing time limited its real-time applicability. Random Forest, ANN, and XGBoost consistently delivered robust accuracy across both datasets. In contrast, Logistic Regression and SVM showed moderate performance, with lower accuracy on complex attack types like Exploit.

Finally, the computational efficiency of the models was analyzed through training and testing times (see Table 4). Testing time is critical for real-time applications, and XGBoost, ANN, and Random Forest stood out for their consistently low testing times across both datasets, making them practical choices for real-time anomaly prediction. The stacking model also demonstrated competitive testing times, combining efficiency with enhanced performance. Conversely, KNN and SVM exhibited significantly higher testing times, limiting their suitability for real-time scenarios.



	XGBoost	RF	LR	KNN	ANN	SVM	Proposed
Fuzzers	0,6875	0,7091	0,7143	0,8796	0,6836	0,7141	0,7557
Exploit	0,8394	0,8855	0,7086	0,913	0,866	0,6866	0,8778
Shellcode	0,8359	0,8457	0,7763	0,9657	0,8242	0,7723	0,9164
Worms	0,9653	0,9865	0,9358	0,995	0,9764	0,9372	0,9922
DoS	0,8589	0,8516	0,805	0,9138	0,8609	0,8453	0,8634
Reconnaissance	0,8094	0,878	0,7422	0,9754	0,8588	0,7388	0,8977
Backdoor	0,89	0,8992	0,8051	0,9865	0,8929	0,8038	0,9184
Analysis	0,9109	0,9108	0,8191	0,9893	0,9041	0,8116	0,9166
Generic	0,9911	0,9921	0,9755	0,9872	0,9904	0,9846	0,9911

(a)

	XGBoost	RF	LR	KNN	ANN	SVM	Proposed
Fuzzers	0,8811	0,9071	0,8164	0,8763	0,9233	0,8002	0,9348
Exploit	0,8487	0,8738	0,7408	0,8395	0,8966	0,7894	0,9081
Shellcode	0,9326	0,9535	0,8817	0,9669	0,9532	0,8566	0,9792
Worms	0,9526	0,9771	0,8683	0,9774	0,9865	0,8939	0,9907
DoS	0,9244	0,9328	0,6876	0,9097	0,9129	0,7955	0,943
Falsification	0,9985	0,9996	0,9546	0,995	0,9959	0,9386	0,9996

(b)

FIGURE 8. The overall performance of ML models based on different types of attacks running on: (a) UNSW-NB15 dataset, (b) the new medical dataset for anomaly prediction.

This higher computational cost was a key reason for excluding KNN and SVM from the stacking model, as the focus was on achieving a balance between speed and reliability.

2) REAL-TIME PREDICTION PHASE

In this phase, we assess the real-time prediction capabilities of machine learning models on medical messages from a newly developed medical dataset designed for anomaly detection. A total of 100 sequential messages were tested, comprising 25 normal messages and 75 anomalies distributed across six attack types: 10 Fuzzers attacks, 10 Exploit attacks, 10 Worm attacks, 10 Shellcode attacks, 15 DoS attacks, and 20 Falsification attacks. These messages were transmitted within the designed real-world-inspired scenario to replicate real-world conditions. For Falsification and DoS attacks, the attacks were dynamically generated during data transmission to mimic real-time scenarios where data streams are intercepted, altered, or overwhelmed. The remaining attacks were pre-prepared with attack values inspired by the UNSW-NB15 dataset and transmitted through the network. This comprehensive setup provided a realistic simulation of both normal and anomalous data exchanges, enabling a thorough evaluation of each model's ability to predict anomalies in real-time.

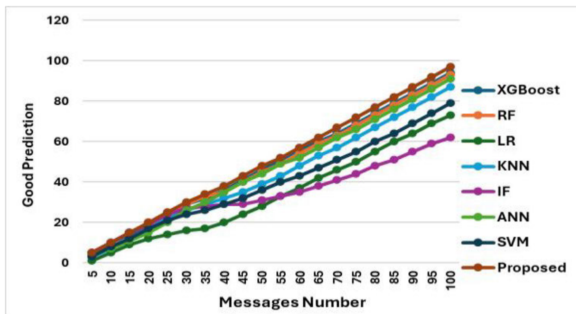


FIGURE 9. Number of good predicted messages by ML models in real-time.

Fig. 9 illustrates the performance of the machine learning models in real-time binary classification, distinguishing between normal and anomalous data across the 100 messages. The proposed stacking model outperformed all others, correctly predicting 97 messages. This exceptional performance underscores its ability to integrate the strengths of its base models, ensuring accurate detection of both normal and anomalous patterns. XGBoost followed closely with 94 correct predictions, demonstrating robust handling of both normal and attack data. Similarly, Random Forest achieved 93 correct predictions, highlighting its reliability in real-time anomaly detection. KNN and ANN also delivered strong results. KNN excelled in identifying normal data, and accurately predicting all 25 normal messages, while ANN maintained consistent performance across all message types. These results position both models as promising candidates for real-time anomaly detection. In contrast, SVM struggled with predicting attack types, reflecting its limitations in handling diverse patterns. Logistic regression underperformed, correctly predicting only 73 messages. Its linear nature restricts its ability to model complex, non-linear relationships, which is evident in its weaker performance with anomalies. Isolation Forest also faced challenges, accurately detecting 24 out of 25 normal messages but identifying only

TABLE 5. Comparison of anomaly detection systems based on ML approaches on IoT and IoMT networks.

Ref	Algorithms or Models	DataSet	IoT Application	Detected Attacks	Effectiveness					Efficiency		Real-time Prediction
					Accuracy	Precision	Recall	F1-Score	FPR	Training Time (s)	Testing Time (s)	
[8]	RF, LOF, IF, SVM, KNN	MIT- BIH	Healthcare	-	-	-	-	-	-	-	-	-
[9]	LR, XGBoost, RF, DT	Medicare Dataset(CMS) PrivateDataset (COIDA)	Healthcare	-	Yes	Yes	Yes	-	-	-	-	-
[10]	K-means, K-medoids partitioning	Collect its own dataset	Healthcare	-	Yes	-	-	-	-	Yes	Yes	-
[11]	R-FCVM	Collect its own dataset	Medical IoT	Replay attacks, Shoulder-surfing attacks, Malware attacks.	Yes	-	-	-	-	-	Yes	-
[12]	Ensemble learning (Stacking, Bagging, Boosting)	WUSTL-EHMS-2020	Medical IoT	Spoofing, Data injection	Yes	Yes	Yes	Yes	-	-	-	-
[14]	CNN1D, CNN2D,CNN3D	BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-23 intrusion detection datasets	IoT	DoS, DDoS, Scan, Theft, Mirai, MITM, MQTT Brute-Force, Sparta SSH Brute-Force, Agressive Scan, UDP Scan, File download, Heartbeat, C&C, Torri, Port Scan, Okiru	Yes	Yes	Yes	Yes	-	-	-	-
[15]	LR, SVM, NB, DT, NN, OCSVM_P, OCSVM_P, EE, ISOF, LOF	NSL-KDD, UNSW-NB15, CICIDS2017	IoT	DDoS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-
[17]	Deep autoencoder	Detection of IoT Botnet attacks	IoT	DDoS: UDP, TCP, SYN	-	-	-	-	Yes	-	-	-
[18]	semi-supervised deep extreme learning machine (SDELM)	UNB-ISCX	IoT	DDoS: UDP Floodign attacks	Yes	Yes	Yes	-	Yes	-	-	-
[19]	KNN, SVM, DT, RF, DNN	Synthetic Dataset	IoT	DDoS: TCP SYN Flood, UDP Flood, HTTP GET Flood	Yes	Yes	Yes	-	Yes	-	-	-
[20]	ANN, DT, KNN, NB, RF, SVM, CNN, EM, k means, SOM	CICIDS2017	IoT	BENIGN, Brute Force, XSS, SQL Injection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-
[23]	SVM_PCA, SVM_NN, SVM_PCA_NN	IoT_Botnet, IoT_Fridje	IoT, SmartHome	DoS, DDoS, XSS, Backdoor, Injection	Yes	Yes	Yes	Yes	-	-	-	-

TABLE 5. ***(Continued.)*** **Comparison of anomaly detection systems based on ML approaches on IoT and IoMT networks.**

[24]	LR, SVM, DT, RF, ANN, OLWPR	collected in Intel Berkeley Research Lab (IBRL) from 54 mica sensors.	IoT	-	Yes	Yes	Yes	Yes	-	-	-	-
[25]	LR, ANN	DS2OS traffic traces	IoT	DoS, Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying, Wrong Setup	Yes	Yes	Yes	Yes	-	-	-	-
[26]	KNN, QDA, Iterative Dichotomiser ID3, RF, AdaBoost, MLP, NB	Bot-IoT	IoT	Probing attacks, DoS, Information Theft.	Yes	Yes	Yes	-	-	Yes	Yes	-
[27]	DT, Adaboost, RF, Gboost, Ensemble learning	Bitcoin transaction data	-	-	Yes	Yes	Yes	-	Yes	-	-	-
Ours	**XGBoost, ANN, RF, IF, LR, KNN, SVM, STACKING**	**UNSW-NB15, New medical dataset with attacks**	**Medical IoT**	**Fuzzers, Exploit, Shellcode,Worms ,Reconnaissance, DoS, Backdoor, Analysis, Generic, Falsification**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

TABLE 6. **Training and testing time of LM anomaly prediction models.**

	New medical dataset for anomaly detection		UNSW-NB15 dataset	
Model	Training time (s)	Testing time (s)	Training tine (s)	Testing time (s)
RF	12.1688	0.2473	8.7314	0.2338
XGBoost	62.8170	0.0327	41.9799	0.1548
KNN	0.9465	59.3154	0.3626	38. 0637
ISOF	1.3206	0.2821	1.0107	0.1428
ANN	110.4858	0.0298	78.0247	0.0396
LR	0.6420	0.0051	0.3793	0.0031
SVM	1059.96	54.5325	901.3636	32. 6092
Proposed	64.22	0.3016	52.657	0.3016

36 anomalies. Its reliance on outlier detection makes it less effective for subtle or nuanced attack patterns.

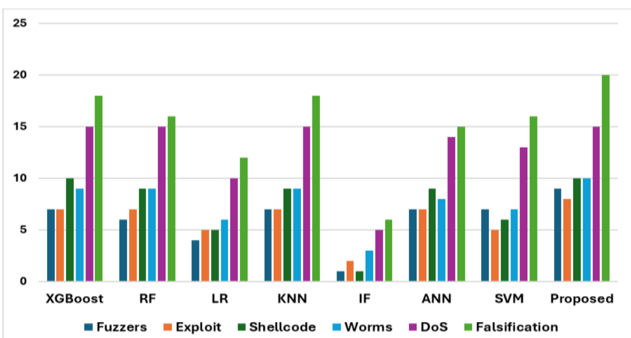


FIGURE 10. **Number of correctly predicted attack types by ML models in real-time.**

For multiclass classification, the models were evaluated on their ability to predict anomalies across the six attack categories, as shown in Fig. 10. The proposed stacking model again emerged as the top performer, accurately detecting 9 Fuzzers, 8 Exploits, 10 Shellcodes, 10 Worms, 15 DoS attacks, and 20 Falsification attacks. Its superior performance stems from its ability to combine the strengths of its base models, enabling it to identify both straightforward and complex attack patterns effectively. XGBoost, Random Forest, and ANN also delivered robust results, demonstrating their capability to handle diverse attack types. KNN achieved prediction accuracy comparable to XGBoost and excelled in detecting closely grouped attack patterns, such as 15 DoS and 18 Falsification attacks. However, KNN's high computational cost during testing limits its suitability for real-time applications, as slower performance can hinder its effectiveness in dynamic environments. Logistic regression and Isolation Forest continued to struggle with complex attack patterns, further highlighting their limitations.

Overall, the results confirm the effectiveness of the proposed stacking model and the value of the newly developed medical dataset. During the pretraining phase, almost all the models showed better performance on the medical dataset compared to UNSW-NB15, demonstrating that the customized attack types improved the models' ability to detect anomalies more accurately. The stacking model consistently outperformed individual models, benefiting from the complementary strengths of XGBoost, Random Forest, and ANN. This trend held in the real-time prediction phase, where the stacking model successfully detected 97 out of 100 messages and achieved high accuracy across all six attack categories. These results not only highlight its robustness in complex, multiclass scenarios but also prove its practical applicability in real-time healthcare environments. In contrast, simpler models like Logistic Regression and Isolation Forest struggled to generalize to nuanced attack patterns. These findings emphasize the importance of tailored datasets, ensemble learning, and efficient real-time processing in building reliable security systems for IoMT infrastructures.

V. CONCLUSION

This research presents a novel real-time anomaly detection model designed for Internet of Medical Things (IoMT) systems, addressing critical cybersecurity challenges through a machine learning-based approach. A new medical dataset was developed, combining physiological data from the BRFSS dataset and attack patterns inspired by the UNSW-NB15 dataset. Additionally, healthcare-relevant attacks were generated to simulate real-world anomalous scenarios in IoMT environments. The new dataset demonstrated superior effectiveness for anomaly detection, significantly improving model performance compared to the UNSW-NB15 dataset.

The proposed stacking ensemble model, integrating XGBoost as the meta-learner with Random Forest and ANN as base models, achieved outstanding results. On the new medical dataset, it attained an accuracy of 98.02%, outperforming other models' accuracy. Real-time prediction analysis further validated the model's robustness, with 97 out of 100 messages correctly classified. These findings underscore the value of the new medical dataset in enhancing anomaly detection capabilities. By incorporating healthcare-relevant attacks and leveraging key features from the UNSW-NB15 dataset, the dataset provides a realistic and challenging environment for training and testing machine learning algorithms. This study highlights the potential of ensemble learning techniques and tailored datasets to significantly advance IoMT security, offering a robust solution for real-time anomaly detection in critical healthcare systems.

This research work has a few limitations that open directions for future research. First, the dataset used includes a limited set of attack types, which may not reflect all possible or newly emerging threats. A possible future direction could be to expand the dataset with more recent attacks or to explore reinforcement learning techniques that allow the model to adapt dynamically to unknown or evolving attack patterns. Second, the evaluation was done only on a custom medical dataset, which limits the ability to assess how well the models perform in other environments. Future studies could involve evaluating the models on other public benchmark datasets to better assess their generalizability.

APPENDIX

See Table 5.

ACKNOWLEDGMENT

The authors would like to thank Dr. Franjieh El Khoury for her valuable comments and proofreading of this article.

REFERENCES

[1] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," *Healthcare Informat. Res.*, vol. 22, no. 3, p. 156, 2021, doi: 10.4258/hir.2016.22.3.156.

[2] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. P. Thipperudraswamy, "Artificial intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare," *Biosensors*, vol. 12, no. 8, p. 562, Jul. 2022, doi: 10.3390/bios12080562.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Jul. 2018, doi: 10.1155/2018/5978636.

[4] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019, doi: 10.1109/COMST.2019.2914094.

[5] T. Levy-Loboda, E. Sheetrit, I. F. Liberty, A. Haim, and N. Nissim, "Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms," *J. Biomed. Informat.*, vol. 132, Aug. 2022, Art. no. 104129, doi: 10.1016/j.jbi.2022.104129.

[6] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102685, doi: 10.1016/j.adhoc.2021.102685.

[7] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/7348942

[8] E. Šabić, D. Keeley, B. Henderson, and S. Nannemann, "Healthcare and anomaly detection: Using machine learning to predict anomalies in heart rate data," *AI Soc.*, vol. 36, no. 1, pp. 149–158, May 2020, doi: 10.1007/s00146-020-00985-1.

[9] S. Park, K. H. Lee, B. Ko, and N. Kim, "Unsupervised anomaly detection with generative adversarial networks in mammography," *Sci. Rep.*, vol. 13, no. 1, pp. 1–10, Feb. 2023, doi: 10.1038/s41598-023-29521-z.

[10] M. Kavitha, P. V. V. S. Srinivas, P. S. L. Kalyampudi, S. F. Choragudi, and S. Srinivasulu, "Machine learning techniques for anomaly detection in smart healthcare," in *Proc. 3rd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Sep. 2021, pp. 1350–1356.

[11] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A practical model based on anomaly detection for protecting medical IoT control services against external attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/TII.2020.3011444.

[12] T. Alsolami, B. Alsharif, and M. Ilyas, "Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the Internet of Medical Things," *Sensors*, vol. 24, no. 18, p. 5937, Sep. 2024, doi: 10.3390/s24185937.

[13] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

[14] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[15] S. Das, M. Ashrafuzzaman, F. T. Sheldon, and S. Shiva, "Ensembling supervised and unsupervised machine learning algorithms for detecting distributed denial of service attacks," *Algorithms*, vol. 17, no. 3, p. 99, Feb. 2024, doi: 10.3390/a17030099.

[16] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[17] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-Based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

[18] N. Ravi and S. M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[19] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.

[20] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[21] K. Choi, J. Yi, C. Park, and S. Yoon, "Deep learning for anomaly detection in time-series data: Review, analysis, and guidelines," *IEEE Access*, vol. 9, pp. 120043–120065, 2021, doi: 10.1109/ACCESS.2021.3107975.

[22] B. Luo, H. Wang, H. Liu, B. Li, and F. Peng, "Early fault detection of machine tools based on deep learning and dynamic identification," *IEEE Trans. Ind. Electron.*, vol. 66, no. 1, pp. 509–518, Jan. 2019, doi: 10.1109/TIE.2018.2807414.

[23] G. Abdelmoumin, D. B. Rawat, and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4280–4290, Mar. 2022, doi: 10.1109/JIOT.2021.3103829.

[24] I. G. A. Poornima and B. Paramasivan, "Anomaly detection in wireless sensor network using machine learning algorithm," *Comput. Commun.*, vol. 151, pp. 331–337, Feb. 2020, doi: 10.1016/j.comcom.2020.01.005.

[25] J. Alsamiri and K. Alsubhi, "Internet of Things cyber attacks detection using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, 2019, doi: 10.14569/ijacsa.2019.0101280.

[26] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," *Blockchain, Res. Appl.*, vol. 5, no. 3, Sep. 2024, Art. no. 100207, doi: 10.1016/j.bcra.2024.100207.

[27] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Trans. Inf. Theory*, vol. IT-13, no. 1, pp. 21–27, Jan. 1967, doi: 10.1109/TIT.1967.1053964.

[28] S. A. Mulay, P. R. Devale, and G. V. Garje, "Intrusion detection system using support vector machine and decision tree," *Int. J. Comput. Appl.*, vol. 3, no. 3, pp. 40–43, Jun. 2010, doi: 10.5120/758-993.

[29] G. J. M. Rosa, "The elements of statistical learning: Data mining, inference, and prediction by HASTIE, T., TIBSHIRANI, R., and FRIEDMAN, J.," *Biometrics*, vol. 66, no. 4, p. 1315, Dec. 2010, doi: 10.1111/j.1541-0420.2010.01516.x.

[30] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Proc. Comput. Sci.*, vol. 89, pp. 213–217, Jun. 2016.

[31] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T. Liu, "LightGBM: A highly efficient gradient boosting decision tree," in *Proc. Adv. Neural Inf. Process. Syst.*, Dec. 2017, pp. 3146–3154.

[32] A. Kuri, "The best neural network architecture," in *Proc. Mex. Int. Congr. Artif. Intell.*, Monterrey, Mexico, Oct. 2014, pp. 24–29.

[33] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance Internet of Things' devices security," *Sensors*, vol. 23, no. 12, p. 5568, Jun. 2023, doi: 10.3390/s23125568.

[34] (2015). *Centers for Disease Control and Prevention (CDC) (2015) Behavioral Risk Factor Surveillance System (BRFSS) Dataset*. Accessed: Dec. 2024. [Online]. Available: https://www.cdc.gov/brfss/

[35] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

[36] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," in *Proc. Int. Conf. Signal Process. Commun. Eng. Syst.*, Jan. 2015, pp. 92–96.

[37] B. Alsharif, M. Alanazi, and M. Ilyas, "Machine learning technology to recognize American sign language alphabet," in *Proc. IEEE 20th Int. Conf. Smart Communities, Improving Quality Life Using AI, Robot. IoT (HONET)*, Dec. 2023, pp. 173–178, doi: 10.1109/HONET59747.2023.10374964.

HADJER GOUMIDI received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Ferhat Abbas University, Setif 1, Algeria, in 2014, 2016, and 2021, respectively. She is currently pursuing the Ph.D. degree in computer engineering with Polytechnique Montréal, Montreal, QC, Canada. Her research interests include data security and privacy in the IoT networks and healthcare systems.

SAMUEL PIERRE (Senior Member, IEEE) is currently a Professor with the Department of Computer and Software Engineering, Polytechnique Montréal, Canada, and the Director of the Mobile Computing and Networking Research Laboratory (LARIM). He has authored or co-authored more than 600 technical publications, including articles in refereed archival journals, textbooks, patents, and book chapters. His research interests include wired and wireless communications, mobile computing and networking, cloud computing, and e-learning. He was a fellow of the Engineering Institute of Canada, in 2003, and the Canadian Academy of Engineering, in 2008. In December 2011, he was appointed as a member of the Order of Canada. He was a recipient of several awards, including the Prix Poly 1873 for excellence in teaching and training, in 2001 and 2005, and the Knight of the National Order of Quebec, in 2009. In May 2014, he was a recipient of an Honorary Doctorate from the University of Quebec at Trois-Rivières (UQTR) and another from the University of Quebec in Outaouais (UQO), in November 2016. In 2017, he received the El Fassi Prize from the Agence universitaire de la Francophonie (AUF) to highlight the action of a person who has exerted a significant influence through the quality of his expertise and the innovative nature of his achievements at the international level in the fields of research, training, development and international cooperation, governance and/or transfer of knowledge or skills. He received the Grand Prize for Professional Excellence from the Order of Engineers of Quebec, in 2020, the Gold Medal from Engineers Canada, in 2021, the Promotion of Officer of the National Order of Quebec, in 2022, the JM Ham Award from IEEE Canada, in 2023, for "outstanding contributions to training the next generation of scientists and engineers in the areas of mobile computing, networking, and e-learning," and the Julian C. Smith Medal of the Engineering Institute of Canada "for distinguished achievements in the development of Canada," in 2024.