Journal of Systems Engineering and Information Technology (JOSEIT)
Volume 4, No. 2, September (2025), Pages 42-50
e-ISSN: 2829-310X | 10.29207/joseit.

Towards Effective Classification of Intrusion in Internet of Medical Things using Random Forest Classifier for Sustainable Health Care

Jimoh R.G[1], Oyelakin A.M[2*], Sanni S.A[3], Salau-Ibrahim T.T[4], Akanbi M.B[5], Saka B.A[6], Lasisi I.O[7], Ibrahim T.L[8]

[1]Department of Computer Science, University of Ilorin, Ilorin, Nigeria
[2,6,7]Department of Computer Science, Crescent University, Abeokuta, Nigeria
[3]Department of Computer Science, University of Eswatini, Kwaluseni, The Kingdom of Eswatini
[4]Department of Cyber Security, Federal University of Lafia, Nigeria
[5]Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria
[8]Department of Paediatrics, Federal University of Lafia, Nigeria

[*]*moruff.oyelakin@cuab.edu.ng*

Abstract. Information Technology is extensively utilized in contemporary healthcare settings. Nevertheless, healthcare facilities are frequently targeted by malicious actors aiming to disrupt services and exfiltrate sensitive data. Intrusion detection systems play a crucial role in monitoring and analyzing computer systems or networks for indications of such attacks. To safeguard healthcare technologies, including the Internet of Medical Things (IoMT), it is imperative to protect them from these threats. Machine learning models have demonstrated superiority over traditional methods in detecting intrusions. However, some of these models still exhibit limitations, such as generating false alarms when identifying attacks on IoMT. Consequently, the development of more accurate models for detecting these attacks is essential. Security experts have developed datasets that simulate various attack scenarios for testing purposes, one of which is the IoMT Attack Testbed. This study proposes a three-step methodology for constructing an effective intrusion detection model. It employs a Random Forest classifier to categorize intrusions within the dataset. Through dataset analysis, the study provides insights into feature handling, addresses data imbalance issues, and identifies significant features for the model. The model's parameters were optimized to enhance its performance. The model was evaluated in two scenarios, with results indicating superior performance in the second scenario when data imbalance was addressed, critical features were selected, and parameters were fine-tuned.

Keywords: *Medical IoT, Medical Data, Machine Learning, Intrusion, Classification*

How to cites:
Jimoh, R., Oyelakin, A., Sanni, S., Salau-Ibrahim, T., Akanbi, M., Saka, B., Lasisi, I., & Ibrahim, T. (2025). Towards Effective Classification of Intrusion in Internet of Medical Things using Random Forest Classifier for Sustainable Health Care. Journal of Systems Engineering and Information Technology (JOSEIT), 4(2). https://doi.org/10.29207/joseit.v4i2.6984

Received by the Editor: 2025-07-20
Final Revision: 2025-09-21
Published: 2025-09-22

SDGs contributed:

© The Author(s) 2025| This is an open-access article under the CC BY 4.0 License
Publisher: Ikatan Ahli Informatika Indonesia

1. Introduction

The Internet of Things (IoT) encompasses the integration of interconnected digital entities, including sensors and processing units [1]. The rapid proliferation of IoT devices has significantly expanded the potential attack surface, thereby facilitating more severe cyber-attacks by malicious actors [2]. For example, certain intruders attempt to deplete the resources of target IoT networks through malicious activities, employing various forms of malware within cyberspace and computer networks [3]. Intrusion detection refers to the systematic monitoring and analysis of events or threats within a computer system or network to identify potential security incidents. Several datasets have been made available for benchmarking security models in the IoT domain, with notable examples being [2], [4], among others.

A study highlighted that the advent of the Internet of Things (IoT) has facilitated more straightforward communication between machines and humans [5]. Furthermore, IoT applications are reportedly transforming various sectors, including healthcare, agriculture, and transportation, thereby significantly impacting our professional and personal lives. Additionally, IoT offers numerous benefits and opportunities for knowledge sharing, innovation, and advancement [6]. [7] contended that although numerous machine learning (ML) studies have been proposed for the development of intrusion detection systems, some still exhibit high false positive rates.

Indeed, various types of malwares have been employed to launch cyber-attacks, often utilizing detection-evasive techniques to avoid being identified [3]. Consequently, the assertion by [8] that Artificial Intelligence and Machine Learning have shown considerable promise in addressing challenges within the healthcare sector through intelligent methodologies is particularly pertinent in mitigating cyber threats.

As highlighted by [9], safeguarding sensitive patient data and ensuring the integrity of devices and networks that underpin the Internet of Medical Things (IoMT) is crucial. Building on this premise, the present study aims to employ a multi-stage approach to enhance machine learning-based intrusion detection models within IoT networks. The innovative methodologies proposed in this research are designed to develop a robust RF-based intrusion classification model capable of generalizing effectively. Specifically, the objective is to construct an intelligent model that can accurately classify intrusions within the selected IoMT attack dataset through comprehensive exploratory data analysis (EDA), feature preprocessing, class balancing, feature selection, and model hyperparameter tuning. The chosen dataset encompasses health attributes and network features. Two scenarios are considered: the first involves constructing an RF-based intrusion classification model without class balancing, feature selection, and hyperparameter tuning of the learning algorithm, while the second incorporates these techniques. In summary, the overarching aim of this paper is to contribute to the development of more robust and accurate intrusion classification models in IoMT, thereby enhancing their performance on unseen data.

A study proposed machine learning (ML)-based methodologies for detecting attacks within Internet of Things (IoT)-based Smart Home Environments, utilizing both single and ensemble classifiers [10]. The selected classifiers were integrated with a meta-heuristic feature selection algorithm. The authors contended that the innovative approaches to dataset cleaning, feature selection, and attack classification contributed to achieving promising outcomes, with Random Forest demonstrating marginally superior performance across all selected metrics. In a related study, [11] employed the K-means algorithm to categorize devices into predefined groups based on their attack sensitivity values within the IoT environment. The researchers asserted that the developed model achieved favorable results across all evaluation metrics. Furthermore, it was noted that the study laid a solid foundation for enhancing the precision of attack detection and protection.

Another study introduced a shallow neural network designed to detect representative attacks within a communication network [12]. The authors proposed an enhanced attack-sharing loss function to address the challenge of imbalanced learning. They demonstrated that their proposed solution could detect network attacks with an F1 score exceeding 99% for various attacks in IoT device communication. In a related study, [13] developed an intrusion detection system aimed at identifying anomalous network traffic in IoT environments. The authors employed the Binary Grey Wolf Optimizer (BGWO) heuristic algorithm and subsequently applied recursive feature elimination (RFE) to select the most relevant feature subset for the target class. Given the dataset's significant class imbalance, the Synthetic Minority Oversampling Technique (SMOTE) was utilized to oversample the minority class. The pre-processed data were then classified using XGBoost. The researchers contended that their proposed method achieved favorable results in terms of accuracy, precision, recall, and F1 score based on the datasets employed.

The methodology proposed by [14] involves the development of a hybrid model that integrates enhanced residual network blocks with bidirectional gated recurrent units. This research primarily focuses on constructing attack classification models for the early detection of attacks across two distinct scenarios. Additionally, [15] introduced a deep learning-based ensemble classification approach aimed at detecting malware in IoT devices. This model employs a three-step process. Initially, data undergoes pre-processing through scaling, normalization, and de-noising. In the subsequent step, feature selection is performed, and one-hot encoding is applied. Finally, in the third step, ensemble classifiers, specifically Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), are utilized for classification. The study reported an average accuracy of 99.5%.

Machine learning models were developed for the classification of attacks within an IoT network. Five supervised learning models were constructed, tested, and evaluated using the IoTID20 dataset [16]. The selected algorithms included Shallow Neural Networks (SNN), Decision Trees (DT), Bagging Trees (BT), K-nearest neighbor (KNN), and Support Vector Machine (SVM). The authors reported that their experimental evaluation achieved an accuracy of 100% for detection in all instances. In a related study, [17] developed a model for detecting attacks in IoT smart applications using a machine learning approach. The authors utilized a public dataset named AWID for evaluation purposes. The study highlighted the promising performance of the t-test technique employed for selecting a reduced number of attributes. It was argued that the approach achieved an accuracy of 99% using only eight features. Furthermore, the authors asserted that the technique demonstrated excellent performance when compared with similar studies.

A Hybrid Intrusion Detection (HID) system was developed utilizing machine learning algorithms, including Random Forest, XGBoost, Decision Tree, K-Nearest Neighbors, and a misuse detection technique [18]. The authors employed the NSL-KDD and CSE-CIC-IDS2018 datasets to evaluate the performance of these algorithms. The study demonstrated promising results across all evaluation metrics. In a related study, [19] proposed a framework for detecting malicious network traffic, employing Support Vector Machine (SVM), Gradient Boosted

Decision Trees (GBDT), and Random Forest (RF) algorithms. It was reported that the model utilizing the RF learning algorithm achieved an accuracy of 85.34%. Furthermore, [20] constructed four distinct models from the dataset using the following learning algorithms: RF, KNN, SVM, and Artificial Neural Network (ANN). The authors contended that the classification of attacks yielded promising results with the four selected algorithms.

Recent studies have introduced novel methodologies to enhance the efficacy and implementation of anomaly-based Intrusion Detection Systems (IDSs) in real-world networks by investigating the application of machine learning models for anomaly-based intrusion detection [21]. This research examined various neural network architectures, including Multilayer Perceptron (MLP), Autoencoders, and Deep Belief Networks (DBN), to evaluate their effectiveness in identifying different types of attacks, such as Denial of Service (DoS) and Brute Force Attacks. The author proposed a three-step approach for intrusion detection, which achieved a classification accuracy of 94.44% on the KDD Cup 99 dataset and 88.39% on the NSL-KDD dataset, with low false-positive rates. However, the datasets employed in this study are outdated compared to more recent datasets that capture contemporary attack representations. Consequently, the model may not generalize effectively to recent, unseen attack datasets.

2. Methods

This study employs a three-stage machine learning approach to develop an intelligent intrusion classification model, subsequently comparing its performance with recent analogous studies. The research utilizes a dataset derived from security issues within the health Internet of Things environment. This dataset was sourced from an experiment known as the Enhanced Healthcare Monitoring System (EHMS) Testbed, as documented by [20]. The selection of this dataset is motivated by its capacity to facilitate the investigation of attacks targeting both medical biometrics and network data within the testbed, as highlighted by [20]. The ensemble method chosen for this study is the Random Forest classifier, which is a tree-based algorithm. Random Forest is a supervised learning algorithm applicable to classification or regression problems, utilizing a tree-like structure to generate predictions [22].

The primary objective of ensemble methods is to enable decision trees to learn from the errors made by their predecessors. Accordingly, this study aims to examine the performance of a Random Forest (RF)-based model in classifying intrusions within the Internet of Medical Things (IoMT) dataset, both with and without the application of Synthetic Minority Over-sampling Technique (SMOTE), feature selection, and hyperparameter tuning. The dataset was divided using an 85:15 split ratio for the experiments. Figure 1 presents a screenshot of the dataset utilized in the experimentation.

	Dir	Flgs	SrcAddr	DstAddr	Sport	Dport	SrcBytes	DstBytes	SrcLoad	DstLoad	SrcGap	DstGap	SIntPkt	DIntPkt	SIntPktAct	DIntPktAct	SrcJitter	DstJitter	sM
2	->	e	10.0.1.172	10.0.1.150	58059	1111	496	186	276914	92305	0	0	3.582333	1.9015	0	0	2.946239	1.6235	
3	->	e	10.0.1.172	10.0.1.150	58062	1111	496	186	230984	76995	0	0	4.294667	2.9015	0	0	3.091654	2.8625	
4	->	e	10.0.1.172	10.0.1.150	58065	1111	496	186	218470	72823	0	0	4.540667	3.2945	0	0	2.849841	3.1655	
5	->	e	10.0.1.172	10.0.1.150	58067	1111	496	186	203376	67792	0	0	4.877667	3.332	0	0	2.452252	3.257	
6	->	e	10.0.1.172	10.0.1.150	58069	1111	496	186	235723	78574	0	0	4.208333	2.8635	0	0	3.021835	2.8225	
7	->	e	10.0.1.172	10.0.1.150	58074	1111	496	186	191284	63761	0	0	5.186	3.803	0	0	3.666978	3.797	
8	->	e	10.0.1.172	10.0.1.150	58076	1111	496	186	217958	72653	0	0	4.551333	2.841	0	0	3.360778	2.822	
9	->	e	10.0.1.172	10.0.1.150	58078	1111	496	186	244536	81512	0	0	4.056667	2.139	0	0	3.272284	2.018	
10	->	e	10.0.1.172	10.0.1.150	58081	1111	496	186	203989	67996	0	0	4.863	4.17	0	0	1.137211	4.066	
11	->	e	10.0.1.172	10.0.1.150	58084	1111	496	186	235518	78506	0	0	4.212	2.319	0	0	3.300342	2.275	
12	->	e	10.0.1.172	10.0.1.150	58086	1111	496	186	283402	94467	0	0	3.500333	2.8505	0	0	2.491458	2.8065	
13	->	e	10.0.1.172	10.0.1.150	58087	1111	496	186	141103	47034	0	0	7.030333	2.7055	0	0	6.544402	2.6715	
14	->	e	10.0.1.172	10.0.1.150	58089	1111	496	186	235723	78574	0	0	4.208333	2.8555	0	0	2.842504	2.8015	
15	->	e	10.0.1.172	10.0.1.150	58094	1111	496	186	256817	85606	0	0	3.862667	2.834	0	0	2.734343	2.736	
16	->	e	10.0.1.172	10.0.1.150	58095	1111	496	186	256618	85539	0	0	3.865667	2.859	0	0	2.606134	2.672	
17	->	e	10.0.1.172	10.0.1.150	58097	1111	496	186	218422	72807	0	0	4.541667	3.318	0	0	2.194388	3.298	
18	->	e	10.0.1.172	10.0.1.150	58103	1111	496	186	240679	80226	0	0	4.121667	2.345	0	0	3.183501	2.31	
19	->	e	10.0.1.172	10.0.1.150	58105	1111	496	186	116327	38776	0	0	8.527667	7.741	0	0	2.643549	7.644	
20	->	e	10.0.1.172	10.0.1.150	58107	1111	496	186	236434	78811	0	0	4.195667	2.3515	0	0	3.275936	2.3165	
21	->	e	10.0.1.172	10.0.1.150	58112	1111	496	186	236886	78962	0	0	4.187667	2.895	0	0	3.002758	2.835	
22	->	e	10.0.1.172	10.0.1.150	58114	1111	496	186	217799	72600	0	0	4.554667	3.3145	0	0	2.039511	3.3095	

WUSTL_IoMT_Data RAW

Figure 1. Screenshot of the Original IoMT Dataset before Pre-processing

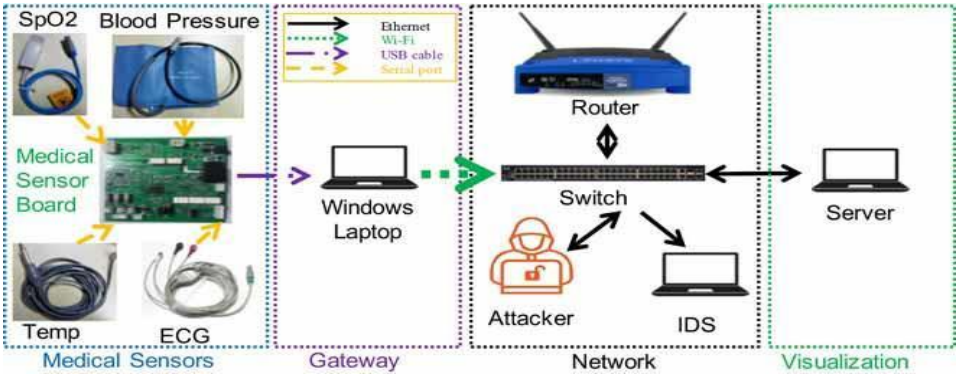

Figure 2. IoMT Attack Testbed [20]

The key stages depicted in Figures 3 and 4 were instrumental in constructing the RF model under varying conditions. As illustrated, the experimental procedures in both scenarios commenced with data collection, followed by exploratory analysis to enhance understanding of the dataset, and data cleaning. Subsequently, attention was directed towards balancing the majority and minority classes using SMOTE, feature selection, and the tuning of the hyperparameters of the RF classifier in the second scenario. The objective is to examine the behavior of the RF-based model when these three critical activities in machine learning-based studies are integrated.

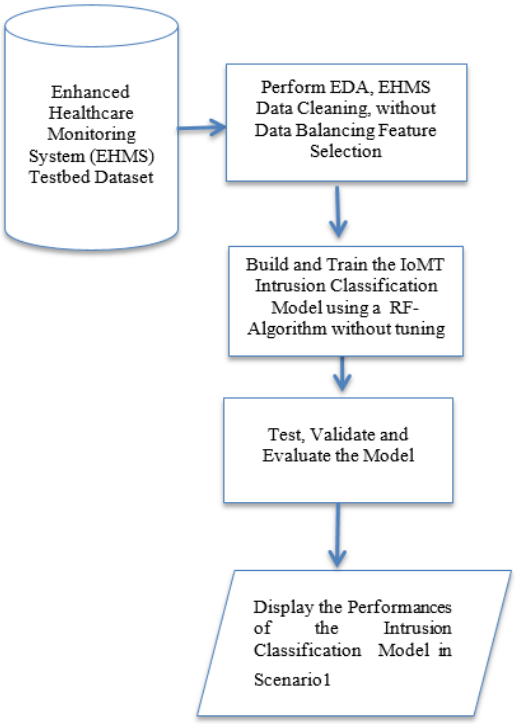

Figure 3. Flow of Activities in the RF-based Intrusion Classification in Scenario1 (Without Class Balancing, Feature Selection and Model Tuning)

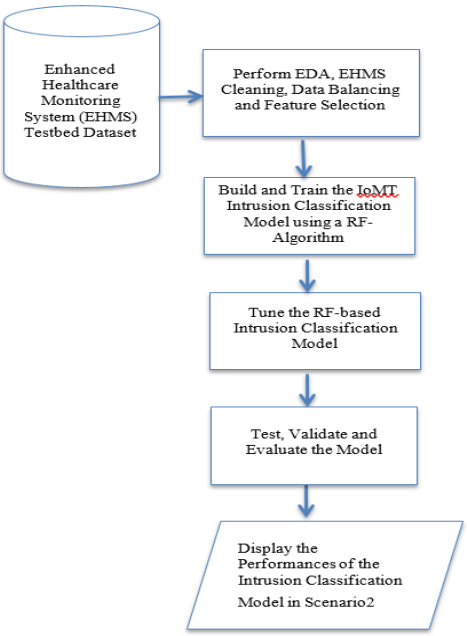

Figure 4. Flow of Activities in the RF-based Intrusion Classification in Scenario 2 (With Class Balancing, Feature Selection and Model Tuning)

2.1 Feature Encoding and Feature Selection Technique used in the Study

The dataset utilized in this study comprises both numeric and non-numeric (object) data types. Consequently, the non-numeric attributes were encoded as part of the data pre-processing measures. The feature encoding was conducted using label encoding. The issue of high-class imbalance within the dataset was addressed through the application of the Synthetic Minority Over-sampling Technique (SMOTE), as proposed by [23]. This technique was employed to rectify the imbalance ratio between the majority and minority classes in the dataset.

Feature selection is recognized as a critical phase in most machine learning (ML)-based classification tasks. For example, [24] demonstrated the significance of selecting promising features in studies employing ML approaches for classification. This study utilized a feature importance method to identify the most promising features that exhibit the strongest relationship with the output variable. Feature importance is a statistical technique that assesses the relative significance of each input variable in predicting the target variable or outcome. It offers insights into which features most significantly influence the model's predictions. A single feature may be utilized in different branches of the tree. In each of the selected ensemble learning classifiers, the feature importance is derived from the feature importance provided by the decision tree as a base classifier. Consequently, the feature importance in the tree-based ensemble can be calculated using equation one.

$$fi_i = \frac{\sum_{j:\text{node j splits on feature i}} ni_j}{\sum_{j\in\text{all nodes}} ni_j} \quad (1)$$

The Random Forest algorithm, introduced by Leo Breiman, addresses various classification and regression challenges [25]. This algorithm is constructed from multiple decision trees utilizing the bagging method, resulting in a homogeneous ensemble. Random Forest operates by averaging numerous deep decision trees, each trained on distinct subsets of the same training dataset, with the objective of minimizing variance. In this study, the hyperparameters of the Random Forest ensemble were meticulously tuned to achieve enhanced results across five selected metrics. The parameters adjusted to optimize model performance included n_estimators, max_depth, min_samples_split, and min_samples_leaf. The significance of this approach lies in its ability to enhance the model's performance.

2.2 Metrics for the Evaluation of the Intrusion Classification Models

The selected metrics for evaluating the model facilitate the identification of an optimal balance to achieve a model with superior performance. The metrics employed include Accuracy, Precision, Recall, F1-Score, and Matthews Correlation Coefficient (MCC). In the context of models, MCC is utilized to assess the contribution of each feature in minimizing prediction error. Equations 2, 3, 4, 5, 6, 7, and 8 delineate the computation of these metrics.

$$P = TP + FN \quad (2)$$

$$N = FP + TN \quad (3)$$

In this context, TP denotes True Positive, FP represents False Positive, FN signifies False Negative, and TN stands for True Negative. A True Positive (TP) occurs when a condition is positive in reality and is accurately predicted as positive. Conversely, a False Positive (FP) arises when a condition is negative in reality but is incorrectly predicted as positive. A True Negative (TN) is identified when a condition is negative in reality and is correctly predicted as negative. Lastly, a False Negative (FN) occurs when a condition is positive in reality but is erroneously predicted as negative.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (5)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (6)$$

$$\text{F1-Score} = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (7)$$

$$\text{MCC} = \frac{\text{TP*TN-FP*FN}}{\sqrt{(\text{TP+FP})*(\text{TP+FN})*(\text{TN+FP})*(\text{TN+FN})}} \quad (8)$$

2.3 Experimental Set Up and Scenarios

All experiments were conducted within the Spyder Python environment on a Windows-based system equipped with a Core i5 processor, a 1TB hard disk drive (HDD), and 8GB of RAM. Various libraries, including pandas, numpy, sklearn, seaborn, Matplotlib, and imblearn, were utilized in the experiments. The study focused on three primary activities aimed at achieving effective classification of intrusions in Medical IoT data: extensive pre-processing, attribute selection, and hyperparameter tuning of the classifier. The pre-processing tasks were meticulously executed based on insights derived from the exploratory analysis of the dataset.

3. Results

This section presents the findings of this study, derived from various experiments conducted in relation to the proposed three-stage RF model for identifying intrusions in IoMT data.

3.1 Dataset Basic Characteristics

The distribution of the samples in the dataset as described by [20] is in Table 1.

Table 1. Dataset Details based on Sample Size

Number of normal samples (non-intrusions)	14,272 (87.5%)
Number of attack samples (intrusions)	2,046 (12.5%)
Total number of samples	16,318

The data presented in Table 1 indicates the presence of a class imbalance issue within the dataset. The exploratory data analysis (EDA) conducted in the Python environment further elucidated the proportions of the majority and minority classes, as depicted in Table 1. Additionally, the results of various EDA activities revealed that the dataset comprises different data types: fifteen (15) features are of the floating-point number data type, twenty-two (22) are non-floating numeric values, and eight (8) attributes are categorical. The significance of conducting EDA on security datasets to enhance the understanding necessary for developing machine learning-based models has been strongly established by [26] and [27]. To facilitate the use of these features in the training and testing of models, preprocessing was performed.

Table 2. The Summary Statistics of the IoMT dataset used in this study.

	Dir	Flgs	...	Attack Category	Label
count	16318.0	16318.000000	...	16318.000000	16318.000000
mean	0.0	3.789190	...	1.818115	0.125383
std	0.0	0.948991	...	0.511686	0.331163
min	0.0	0.000000	...	0.000000	0.000000
25%	0.0	4.000000	...	2.000000	0.000000
50%	0.0	4.000000	...	2.000000	0.000000
75%	0.0	4.000000	...	2.000000	0.000000
max	0.0	6.000000	...	2.000000	1.000000

Table 3. Features in the Dataset After Encoding

	Dir	Flgs	SrcAddr	DstAddr	...	Resp_Rate	ST	Attack Category	Label
0	0	4	0	0	...	0	0.0	2	0
1	0	4	0	0	...	17	0.4	2	0
2	0	4	0	0	...	17	0.4	2	0
3	0	4	0	0	...	17	0.4	2	0
4	0	4	0	0	...	17	0.4	2	0
...	...	...	...	...	...	...	...	...	
16313	0	4	0	0	...	19	0.3	2	0
16314	0	4	0	0	...	19	0.3	2	0
16315	0	4	0	0	...	19	0.3	2	0
16316	0	4	0	0	...	19	0.3	2	0
16317	0	4	0	0	...	19	0.3	2	0

Table 4. Summary of the Dataset Characteristics

Name of the Dataset	Number of Instances in the Dataset	Number of Features in the Dataset	Any Missing/Duplicate Values	Class Distribution	Data Types in the Dataset	Open Issues in the Dataset
WUSTL-EHMS-2020	16318	There are 44 input attributes and one target class that supports binary classification.	No missing values and No Duplicates	Majority Class= 14272 Minority Class= 2046	Mixed Data Types are present in the dataset. Thus, there is need for feature encoding.	The Dataset has class imbalance problem

Following the exploratory data analysis (EDA), the dataset comprises the following features: Columns: [Dir, Flgs, SrcAddr, DstAddr, Sport, Dport, SrcBytes, DstBytes, SrcLoad, DstLoad, SrcGap, DstGap, SIntPkt, DIntPkt, SIntPktAct, DIntPktAct, SrcJitter, DstJitter, sMaxPktSz, dMaxPktSz, sMinPktSz, dMinPktSz, Dur, Trans, TotPkts, TotBytes, Load, Loss, pLoss, pSrcLoss, pDstLoss, Rate, SrcMac, DstMac, Packet_num, Temp, SpO2, Pulse_Rate, SYS, DIA, Heart_rate, Resp_Rate, ST, Attack Category, Label]. The nature of these features necessitated the encoding of certain categorical data to render them suitable for the selected learning algorithms.

3.2 Results of using SMOTE to solve the Class Imbalance Problem in the Dataset

The Synthetic Minority Over-Sampling Technique (SMOTE) was utilized to address the issue of class imbalance within the dataset prior to the classification of intrusions. This procedure was essential to ensure that the constructed model would not exhibit bias. Figure 5 presents a histogram, with the classes depicted in blue, while the synthetically generated samples, aimed at resolving the class imbalance problem, are represented in red.

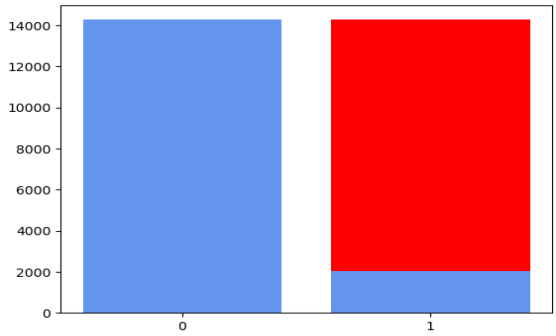

Figure 5. Histogram of Class Imbalance Problem in the Dataset

Table 5 presents the distributions of the dataset as initially observed, as well as before and after the application of SMOTE as a re-sampling technique, as derived from the experimental analyses.

Table 5. Distribution of the Dataset Before and After Applying SMOTE

S/N	Description of the Operations	Size of the Classes in the Dataset
1	Original dataset as obtained from Hady et al. (2020)	{0: 12127, 1: 1743}
2	Before Counter	{0: 12127, 1: 1743}
3	After Counter	{0: 12127, 1: 12127}

Table 6. Classification Results of RF-based Intrusion Classification Model without FS and Hyper-parameter Tuning (Scenario1)

Learning Algorithm\Metrics	Accuracy (%)	Precision	Recall	F1-Score	MCC
Random Forest Algorithm	94.1200	0.9408	0.5248	0.6883	0.6901

Table 6 presents the classification results of the model based on the five selected metrics, utilizing the pre-processed features input into the RF ensemble classifier without feature selection and without hyperparameter tuning. An 85:15 split ratio of the dataset was consistently employed across all experiments.

Table 7. Classification Results of RF-based Intrusion Classification Model with FS and Hyper-parameter Tuning (Scenario2)

Learning Algorithm\Metrics	Accuracy (%)	Precision	Recall	F1-Score	MCC
Random Forest Algorithm	98.53	0.9852	0.9995	0.9123	0.7801

Table 7 presents the classification results of the model based on the five selected metrics, following the selection of the most discriminative features and multiple tuning of the model's hyperparameters. An 85:15 split ratio was consistently employed across all experiments.

4. Discussion

This study presents findings from the application of a Random Forest (RF)-based classifier to detect intrusions within the selected binary class Internet of Medical Things (IoMT) dataset. The methodology employed in this paper is informed by the prevailing scholarly consensus that it is crucial to ensure the accuracy of results derived from an RF-based model. This is achieved by ensuring the model effectively and accurately learns the patterns within the dataset while avoiding data leakage and overfitting. Consequently, this study emphasizes the implementation of comprehensive exploratory data analysis, re-sampling of instances in the highly imbalanced dataset, selection of the most promising attributes using the feature importance method, and tuning of the RF algorithm's hyperparameters in the intrusion classification task.

In the dataset, the features Dir, Flgs, SrcAddr, DstAddr, SrcMac, and DstMac were identified as non-numeric types necessitating encoding. Consequently, all non-numeric features in the dataset were encoded using label encoding as part of the data pre-processing steps implemented in the study. It was observed that, without addressing certain unresolved issues within the dataset, the model's performance in scenario 1 was suboptimal. For the train-test split, 85% and 15% were allocated to the training and testing sets, respectively, across all experiments. The comprehensive exploratory analysis conducted revealed fundamental patterns and characteristics of the dataset.

This analysis further informed the authors on how to effectively utilize the dataset for training and testing attack classification models in the IoMT environment.

It was demonstrated that enhancing the dataset through SMOTE-based resampling, employing Feature Importance as a feature selection technique, and optimizing the hyperparameters of the RF algorithm significantly improved the model's performance in Scenario 2 compared to the overall results in Scenario 1. Following extensive experimentation in both Scenarios 1 and 2, we established a threshold to identify the most promising features in the dataset for constructing and training the RF-based intrusion classification model. These selected features were utilized in the training of the tree-based ensemble model. The performance of the RF-based intrusion classification model is promising and surpasses that of some recent and comparable studies in this security domain.

5. Conclusions

This study conducted an exploratory data analysis (EDA) to elucidate patterns within the selected EMHS dataset, thereby enhancing comprehension. The identified characteristics offered deeper insights into the pre-processing of the dataset's features. Subsequently, the issue of class imbalance observed in the dataset was addressed using the Synthetic Minority Over-sampling Technique (SMOTE). In addition, discriminative features were identified through feature importance within the Random Forest (RF) algorithm, and the hyperparameters of the RF-based intrusion classification model were iteratively optimized. The objective of these three-stage techniques was to ensure that the RF ensemble classifier achieved promising classification outcomes for intrusion detection within the data. Two scenarios were examined: one without and one with the aforementioned three stages. Experimental results demonstrated that employing SMOTE for class balancing, feature selection, and hyperparameter tuning significantly enhanced the performance of the RF-based intrusion detection model compared to the RF-based model without these techniques. It is concluded that the RF-based model can serve as an effective security measure against potential attacks in real-world Internet of Medical Things (IoMT) environments, given its promising results. It is posited that a secure IoMT network will better sustain technology-driven healthcare delivery in both developed and developing nations.

Declaration

The authors declare that there are no known competing interests that could have appeared to influence the work reported in this paper.

References

[1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018.

[2] I. Ullah and Q. H. Mahmoud, "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks," in *Advances in Artificial Intelligence*, vol. 12109, C. Goutte and X. Zhu, Eds., Cham: Springer, 2020, pp. 642–649. doi: 10.1007/978-3-030-47358-7_52.

[3] A. M. Oyelakin, T. T. Salau-Ibrahim, B. S. Ogidan, R. D. Azeez, and I. K. Ajiboye, "Peer-to-Peer Botnets: A Survey of Propagation, Detection and Detection Evasive Techniques," *Fulafia Journal of Science and Technology*, vol. 5, no. 3, pp. 13–18, 2019.

[4] 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.

[5] A. Tasnim et al., "Experimental Analysis of Classification for Different Internet of Things (IoT) Network Attacks Using Machine Learning and Deep Learning," in *Proc. 2022 Int. Conf. Decision Aid Sci. Appl. (DASA)*, 2022, pp. 406–410.

[6] J. Alsamiri and K. Alsubhi, "Internet of Things Cyber-Attacks Detection Using Machine Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 627–634, 2019, doi: 10.14569/IJACSA.2019.0101280.

[7] J. Gu, L. Wang, H. Wang, and S. Wang, "A novel approach to intrusion detection using SVM ensemble with feature augmentation," *Computers & Security*, vol. 86, pp. 53–62, 2019, doi: 10.1016/j.cose.2019.05.022.

[8] T. B. Aremu, A. M. Oyelakin, M. B. Akanbi, H. F. Sulaimon, and K. M. Odeyale, "Machine Learning Techniques for Early Classification of COVID-19 Disease in Patients," *J. Inf. Commun. Technol. Robot. Appl.*, vol. 13, no. 1, pp. 8–14, 2022.

[9] O. Panahi, "Secure IoT for Healthcare," *Eur. J. Innov. Stud. Sustain.*, vol. 1, no. 1, pp. 1–5, 2025, doi: 10.59324/ejiss.2025.1(1).xx.

[10] A. M. Oyelakin et al., "Novel Machine Learning Approaches for Identifying Attacks in IoT-based Smart Home Environment," *Int. J. Wireless Microw. Technol.*, vol. 15, no. 2, pp. 41–50, 2025, doi: 10.5815/ijwmt.2025.02.04.

[11] H. Wang, D. Guo, J. Wei, and J. Li, "A method of classifying IoT devices based on attack sensitivity," *J. Inf. Secur. Appl.*, vol. 82, 2024, Art. no. 103751, doi: 10.1016/j.jisa.2024.103751.

[12] J. Ehmer, Y. Savaria, B. Granado, J.-P. David, and J. Denoulet, “Network Attack Classification with a Shallow Neural Network for Internet and Internet of Things (IoT) Traffic,” *Electronics*, vol. 13, no. 16, Art. no. 3318, 2024, doi: 10.3390/electronics13163318.

[13] B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, “IoT Intrusion Detection System Based on Machine Learning,” *Electronics*, vol. 12, no. 20, Art. no. 4289, 2023, doi: 10.3390/electronics12204289.

[14] H. Yu, C. Kang, Y. Xiao, and Y. Yang, “Network Intrusion Detection Method Based on Hybrid Improved Residual Network Blocks and Bidirectional Gated Recurrent Units,” *IEEE Access*, vol. 11, pp. 68961–68971, 2023, doi: 10.1109/ACCESS.2023.3271866.

[15] S. Riaz et al., “Malware Detection in Internet of Things (IoT) Devices Using Deep Learning,” *Sensors*, vol. 22, no. 23, Art. no. 9305, 2022, doi: 10.3390/s22239305.

[16] A. A. Alsulami, Q. Abu Al-Haija, A. Tayeb, and A. Alqahtani, “An Intrusion Detection and Classification System for IoT Traffic with Improved Data Engineering,” *Appl. Sci.*, vol. 12, Art. no. 12336, 2022, doi: 10.3390/app122312336.

[17] T. Gaber, A. El-Ghamry, and A. E. Hassanien, “Injection Attack Detection Using Machine Learning for Smart IoT Applications,” *Phys. Commun.*, vol. 52, Art. no. 101685, 2022.

[18] F. Alghayadh and D. Debnath, “A Hybrid Intrusion Detection System for Smart Home Security Based on Machine Learning and User Behavior,” *Adv. Internet Things*, vol. 11, pp. 10–25, 2021, doi: 10.4236/ait.2021.111002.

[19] M. Anwer, M. U. Farooq, and S. M. Mahmood Khan, “Attack Detection in IoT Using Machine Learning,” *Eng. Technol. Appl. Sci. Res.*, vol. 11, no. 3, pp. 7273–7278, 2021.

[20] A. A. Hady et al., “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.

[21] M. Labonne, “Anomaly-Based Network Intrusion Detection Using Machine Learning,” *Institut Polytechnique de Paris*, 2020. [Online]. Available: https://theses.hal.science/tel-02988296/file/88255_LABONNE_2020.pdf

[22] P. Koko, M. Zorman, M. M. Stiglic, and I. Malèiae, “The limitations of decision trees and automatic learning in real world medical decision making,” *J. Med. Syst.*, vol. 21, no. 6, pp. 529–533, 1997, doi: 10.3233/978-1-60750-896-0-529.

[23] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: Synthetic Minority Over-sampling Technique,” *J. Artif. Intell. Res.*, vol. 16, pp. 321–357, 2002, doi: 10.1613/jair.953.

[24] A. M. Oyelakin and R. G. Jimoh, “A Survey of Feature Extraction and Feature Selection Techniques Used in Machine Learning-Based Botnet Detection Schemes,” *VAWKUM Trans. Comput. Sci.*, vol. 9, pp. 1–7, 2021. [Online]. Available: https://vfast.org/journals/index.php/VTCS/article/view/604/658

[25] L. Breiman, “Random Forests,” *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001. [Online]. Available: https://www.stat.berkeley.edu/~breiman/randomforest2001.pdf

[26] R. G. Jimoh and A. M. Oyelakin, “On the Comprehensive Analyses of CTU-13 Botnet Dataset for Cyber Security Researches,” *Indones. J. Data Sci.*, vol. 3, no. 1, pp. 13–23, 2025. [Online]. Available: https://ejournal.unjaya.ac.id/index.php/ijds/article/view/1554

[27] A. M. Oyelakin et al., “Overview and Exploratory Analyses of CICIDS 2017 Intrusion Detection Dataset,” *J. Syst. Eng. Inf. Technol. (JOSEIT)*, vol. 2, no. 2, pp. 45–52, 2023, doi: 10.29207/joseit.v2i2.5411.