National College of Ireland

# A Super Learner-Based Framework for Securing Medical IoT Networks Enhanced Intrusion Detection

MSc Research Project
Artificial Intelligence

ANUDEEP YARLAGADDA
Student ID: X23338466

School of Computing
National College of Ireland

Supervisor: SHERESH ZAHOOR

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

**Student Name:** Anudeep Yarlagadda

**Student ID:** X23338466

**Programme:** MSc Artificial Intelligence **Year:** 2024-25

**Module:** MSc (Research) Practicum

**Supervisor:** Sheresh Zahoor

**Submission Due Date:** 11th Aug 2024

**Project Title:** A Super Learner-Based Framework for Securing Medical IoT Networks Enhanced Intrusion Detection

**Word Count:** 7165 **Page Count** 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Anudeep Yarlagadda

**Date:** 8th Aug 2024

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies) | □* |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □* |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □* |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# A Super Learner-Based Framework for Securing Medical IoT Networks Enhanced Intrusion Detection

Anudeep Yarlagadda
Student ID: X23338466

**Abstract**

Intrusion Detection Systems (IDS) are essential for safeguarding Medical Internet of Things (MIoT) networks, which handle sensitive biometric and network data in real-time. Traditional machine learning models like Logistic Regression, SVM, and Naïve Bayes often lack adaptability, accuracy, and explainability when applied to highly imbalanced and complex medical datasets. These limitations include high false negative rates, poor generalization, and limited interpretability. This study introduces a Super Learner-based framework to overcome these challenges using the WUSTL-EHMS-2020 dataset, which contains both biometric and network flow metrics. The proposed Super Learner is a stacking ensemble that combines the strengths of LightGBM, AdaBoost, and Random Forest classifiers. These base models generate out-of-fold predictions through 10-fold cross-validation, which are then stacked and used to train a meta-learner—Gradient Boosting Classifier—ensuring unbiased, high-quality learning. The ensemble structure captures complex patterns and interactions missed by individual models. After preprocessing, balancing with SMOTE, and feature selection, the Super Learner achieved the highest accuracy of 100%, significantly outperforming baseline models. Additionally, Explainable AI techniques like LIME were integrated to interpret predictions and ensure trust and transparency in medical applications. This framework sets a new benchmark in secure, interpretable, and high-performing intrusion detection for medical IoT environments.

Keywords: Medical IoT, Intrusion Detection, Super Learner, Ensemble Learning, Explainable AI.

# 1 Introduction

## 1.1 Aim of the study

The aim of this study is to develop a strong and intelligent IDS specifically designed for medical IoT environments using advanced ML and ensemble techniques. The focus is on accurately detecting cyberattacks that threaten the confidentiality and integrity of sensitive healthcare data. By utilizing the dataset, the study seeks to improve detection accuracy while

maintaining low false positive rates. Additionally, the integration of XAI tools like LIME ensures the system's decisions are transparent and interpretable, making it easy for practical deployment in real-world healthcare settings Vellido (2020).

## 1.2 Research Questions

There are some research questions for this study:

1. How effective are traditional ML models in detecting intrusions within medical IoT environments using the dataset?
2. Can ensemble learning techniques, specifically a Super Learner framework, improve the accuracy of intrusion detection in comparison to individual models?
3. What role does data preprocessing—including outlier removal, normalization, and SMOTE oversampling—play in improving model performance for highly imbalanced medical IoT data?

## 1.3 Objectives of the Research

The objectives of research for this report are:

1. To evaluate and compare the performance of various traditional and ensemble ML algorithms for IDS in medical IoT.
2. To design and implement a Super Learner ensemble model that combines the strengths of multiple base learners and achieves high detection accuracy.

## 1.4 Outline of the Report

This report is structured into the following sections:

- **Chapter 1: Introduction** – Introduces the research problem, aims, research questions, and objectives of the study. It establishes the context of intrusion detection in Medical IoT and highlights the importance of explainable AI in healthcare applications.
- **Chapter 2: Related Work** – Provides a comprehensive review of existing literature on machine learning applications in intrusion detection systems, with a focus on Medical IoT. It compares traditional and contemporary approaches, identifies research gaps, and justifies the chosen methodology.
- **Chapter 3: Research Methodology** – Details the CRISP-DM-based methodology used in the study, including data understanding, preprocessing techniques like normalization and SMOTE, model training strategies, and evaluation metrics.
- **Chapter 4: Design Specification** – Describes the architecture of the proposed system and elaborates on the Super Learner framework. It also discusses the use of Explainable AI techniques for interpretability.
- **Chapter 5: Implementation** – Explains the technical implementation of individual machine learning models.
- **Chapter 6: Evaluation** – Presents the results of model evaluations and it also compares the performance of all models and highlights the superior accuracy and explainability of the Super Learner.
- **Chapter 7: Conclusion and Future Work** – Summarizes the conclusion and future works.

# 2 Related Work

## 2.1 Data Analytics in Intrusion Detection

Data analytics has emerged as a powerful tool Adewusi et al. (2024) in enhancing the capabilities of IDS by enabling them to evolve from static, signature-based mechanisms to dynamic, intelligent detection engines Neupane et al. (2022). The foundation of modern IDS is increasingly data-centric, wherein patterns, correlations, and behavioural anomalies are mined from high-dimensional network traffic data to identify suspicious or malicious activities Adebzadeh et al. (2024). In traditional systems, fixed rules and predefined attack signatures often fail to recognize zero-day exploits or sophisticated intrusion techniques. Data analytics offers a solution by harnessing techniques Sarker (2023). In anomaly-based detection especially, the data analytics can be used to construct behavioural baselines and identifying deviations, which in many cases may be one of the early signs of an intrusion attempt Martins et al. (2022). models of supervised learning have shown to be powerful predictive models when labelled datasets are used to train them. Besides, unsupervised methods such as clustering and dimensionality reduction see application where labelled data is limited, as is often the case in practice. Since detection is only the first step, data analytics enables the derivation of actionable information, including the enumeration of vulnerable endpoints, typical attack vectors, and user actions that assist in security breaches Rajasekar et al. (2022).

## 2.2 Rise of Data Driven Security in Medical IoT

The adoption of data-driven security frameworks in Medical Internet of Things (MIoT) environments has become increasingly necessary due to the unique sensitivity and complexity of medical data and device networks Mudgil et al. (2023). Medical IoT systems, comprising wearables, sensors, remote monitors, and interconnected clinical devices, generate continuous streams of biometric and network traffic data that must be protected against intrusions in real time Stergiou et al. (2023). Unlike traditional IT infrastructures, MIoT systems operate in real-time and are highly decentralized, introducing significant vulnerabilities. Data analytics provides the ability to dynamically detect and respond to these vulnerabilities by analysing large volumes of heterogeneous data to uncover patterns indicative of malicious activity Alzaabi and Mehmood (2024). Several studies have emphasized the need for healthcare-specific intrusion detection models that understand the operational characteristics of medical devices and the contextual meaning of biometric data. To give a few examples, a rise in the data packet rate by a heart monitor may be anticipated during exercise but could indicate spoofing or injection attacks when out of context. This level of subtle interpretation is made possible only with the help of analytics-powered systems. Moreover, the data analytics facilitates cross-layer security, whereby the network, device, and application layer information are combined to model threats comprehensively.

## 2.3 ML Techniques in Intrusion Detection in Medical IoT

The first study given by in Ahmed et al. (2023) focuses on examining how IDS can improve the security of IoMT settings. The rationale is that the study aims to handle essential privacy

and security issues in IoMT, which are caused by the sharing of delicate physiological information through wireless networks and the restricted calculating and energy capabilities of medical gadgets. The authors develop a thorough framework according to which ML-based IDS solutions are considered in terms of the three-layer structure of IoMT perception, network, and application layers. They examine the appropriateness of different ML methods in the detection of attacks including spoofing, eavesdropping, data injection, and denial of service. The methodology additionally evaluates the training sets employed in training IDS models and contrasts the performance of the models based on their results. An important problem that is solved is that it is not possible to deploy traditional cryptographic solutions because of the heterogeneity and resource limitations of devices. As the study concluded, ML-based IDS has potential in identifying both known and unknown threats and has a better adaptability rate across the IoMT layers. Nevertheless, drawbacks are the lack of realistic IoMT-specific data, the large number of false positives in dynamic scenes, and computation costs that make real-time operation on resource-limited devices challenging. Those shortcomings identify the potential of lightweight, explainable, adaptive ML models specific to IoMT as a foundation of the future research directions.

It is suggested by Fouda et al. (2022) that the study develops a new subclass-based IDS to resolve the critical security issues introduced by the hardware, software, and network limitations during the handling of delicate medical information. In order to produce such subclasses, the authors incorporate a dynamic autoencoder (DynAE) deep clustering model, which overcomes the drawbacks of the classical clustering algorithms and leads to more precise and reliable intrusion detection. The approach has been tested on the actual TON_IoT data and compared to a number of the state-of-the-art one-class classifiers. The findings indicate that the suggested Deep SDOSVM is far more accurate and reliable than other current models in detecting network intrusion in IoMT settings. Nevertheless, the use of deep learning models in the approach can cause computational burden, which can make it impossible to use on extremely resource-limited IoMT devices. This accuracy-complexity trade-off indicates that additional optimization is possible or even lightweight versions of the model should be designed.

The paper in Lee et al. (2021) suggests a new Multi-class Classification-based IDS aimed at improving the security of smart healthcare systems in smart cities by precisely detecting and classifying intrusions in medical IoT networks in practice. The objective is to address the shortcoming of the past work which was conducted on simulated dataset, such as NSL-KDD or testbed data consisting of one IoT device, whereas they cannot reflect the realities of a medical setup. The suggested M-IDM architecture is based on convolutional neural networks (CNNs) and is taught using genuine network traffic data recorded by medical gadgets, like electrocardiograms and thermometers, at the National Cancer Centre in South Korea. Model allows the classification of severity of the intrusion according to four levels: critical, major, minor, and informal to respond to the security issue in a nuanced way. M-IDM performance was experimentally compared with traditional ML methods and showed better classification accuracy and robustness. An important issue that it discusses is the discrepancy between the simulated and real medical data in the context of intrusion detection research. Nevertheless, one restraint of the method is that it requires high-quality, real-world labelled data which might not be quickly accessible in every medical establishment, thus hampering the expandability and external validity of the model to dissimilar medical contexts.

Thamilarasu et al. (2020) suggested a new Mobile Agent-Based IDS to safeguard networks of interconnected medical devices against severe security and privacy issues that may cause life-

threatening situations. The suggested hierarchical and autonomous system is based on the machine learning and regression algorithms, which enable the mobile agents to process the distributed data in order to detect the threats in real time. To test the conditions in which the system will work the research simulates a hospital network topology that will include elements such as wireless body area networks and other IoMT devices to recreate a realistic environment to test the performance of the system. The simulations indicate that the suggested IDS can attain high detection rates with computational and resource overheads that are minimal, thus exhibiting its aptitude in medical conditions that have limited resources. Nevertheless, one critical drawback of the method is that it was tested on simulated environments and has not been tested on the unpredictable heterogeneity of actual healthcare networks, which could limit its usefulness in autonomous, heterogeneous hospital environments.

The work in Gupta et al. (2022) considers a Tree classifier dedicated to handle the urgent problem of secure and dependable communication in the connected healthcare setting. The key determinant of this study is to design a secure and effective model that can guarantee patient privacy and safety and handle the large amounts of data generated by IoMT devices. The suggested method is based on the tree-based classification algorithm that is capable of significantly decreasing the dimensionality of input data, thus, speeding up the anomaly detection process without affecting accuracy. The model is suitable to be used in resource-limited IoMT devices due to this lightweight design. Through experiments, it is shown that the system has a high detection accuracy of 94.23% which shows that it performs well in detecting network threats. Nevertheless, the application of only one classification methodology potentially reduces the detection of more advanced or evolved cyberattacks, and its performance in dynamic realistic-time conditions in the healthcare environment has not been confirmed in real-life conditions, which may require additional tests and improvement of hybrid models.

The research in Balhareth and Ilyas (2024) develops to improve the security and inhibit the unauthorized access of sensitive information about the patients that is relayed through vulnerable wireless links. This would allow real time monitoring and identification of malicious traffic on the medical device networks, and the data is analysed at the edge of the network to minimize computation on the IoMT devices. The key problem that is solved is the high detection performance under minimal resource usage, which is important in resource-limited IoMT devices. Nevertheless, the fact that the study is centred on binary classification is a drawback of the study as it limits the model as far as recognizing and distinguishing between various forms of attacks is concerned. The proposed model will be expanded to a multi-class classification system in future and its performance on the real IoMT deployment will be evaluated with various classifiers.

Norouzi et al. (2023) proposed a new security system to secure confidential patient information against cyber-attacks through a proposed hybrid model. The research tackles the issue of finding the balance between strong security and the resource constraints of IoMT devices sufficiently well. Nevertheless, the fact that the model is complemented with offline datasets might be not entirely representative of the dynamic healthcare real-time setting, which can impact generalization. Also, its performance scores are very high, which prompts the question of whether it is overfitted, and therefore it should be assessed in practical IoMT implementations to clarify whether it is practically resilient.

In Awotunde et al. (2023), the study proposes to integrate a multi-level feature selection technique with a fuzzy inference system. The core aim is to improve detection accuracy by optimizing feature selection—an essential factor in building efficient IDS models. The proposed method combines the strengths of filter and wrapper approaches: initially applying correlation-based feature selection using a genetic search algorithm to reduce redundancy, followed by a wrapper-based sequential forward selection to further refine the feature set based on classifier accuracy. The key innovation lies in the hybrid feature selection and fuzzy classification, which collectively enhance detection and interpretability. However, the complexity of integrating multiple selection stages and fuzzy logic may increase computational overhead, which could limit its scalability or suitability for real-time applications in highly resource-constrained IoMT environments.

The paper Jeevaraj (2023) presents a model of intrusion detection in wireless sensor networks (WSNs) to detect abnormal behaviour of sensor nodes and enhance the security of the network with the help of AI-based algorithms, specifically on the detection of intrusions at the early stage. The first is to better forecast and forestall all forms of attacks and aberrations that come about due to climatic fluctuations or improperly handled sensors. The suggested methodology focuses on minimal feature selection that would maximize the efficiency of the model and retain high predictive accuracy. To minimize the computational overhead and to increase the accuracy the system employs Bayesian classifier and enhanced feature selection methods. Preprocessing involves a reduction in the number of attributes used to train the model to just six attributes, and this gives a good performance of 95.8 percent accuracy, 0.958 precision, and 0.989 AUC. The primary contribution of the research is the light, but efficient intrusion detection strategy optimized to WSN settings. Nevertheless, a single classifier (Bayes) is a weakness since it might fail to learn complicated attack patterns compared to ensemble or deep learning-based models. Also, the method has not been tried on a live time or resource-constrained implementation which would help uncover more implementation issues.

At last Zachos et al. (2021) presented research that aims at developing an effective anomaly-based intrusion detection system (AIDS) to be particularly deployed in the Internet of Medical Things (IoMT) networks, that are both heterogeneous and resource-constrained by nature thus especially exposed to the cyber threats. This study aims to help improve the safety of patients and network health by identifying abnormalities using host-based and network-based log collection of IoMT devices and edge gateways. It is based on the idea of applying machine learning (ML) to detect abnormal behaviour but with the computational cost maintained at a level that is reliable to be used in real-time or resource-constrained settings. The performance of 6 well-known ML algorithms was tested to find the best fit in terms of anomaly detection, where Naive Bayes performed with an accuracy of 96.13%, showing that it is a highly performing algorithm despite its simplicity. The principal advantage of this work is the practical design, which provides the joint effectiveness of collecting data and operating the algorithms. Nevertheless, one of the weaknesses is that the comparative performance of all the tested algorithms and real-world deployment cases has not been discussed in detail to prove the model works under various and dynamic threat scenarios in live IoMT systems.

# 3 Research Methodology

## 3.1 Dataset Description

The development of the WUSTL-EHMS-2020 dataset was motivated by the fact that there is a gap in the publicly available datasets that would integrate both network flow metrics and patients (biometric data) in the setting of a medical IoT system a gap that a real-time Enhanced Healthcare Monitoring System (EHMS) testbed was specifically designed to fill. Data collection process starts with medical sensors placed on the body of a patient that constantly measure biometric data and transmit it to the gateway. The data is then transmitted over a network--switches and routers--to the server where it is visualized and monitored in real-time. The data is collected in a form of network flows and biometric data and is saved in CSV format with ARGUS (Audit Record Generation and Utilization System) being used as a data-recording tool. The data consists of 44 features in total: 35 network flow metrics features, eight patient biometric readings features, and one label feature that can take the values normal or malicious to differentiate the normal or malicious instances. Labelling has been performed based on the Source MAC address- entries relating to attacker machines were labelled as 1 (attack), whereas the rest of the entries were designated as 0 (normal). Overall, there are 16, 318 samples, among which 14, 272 (87.5%) are labelled as normal and 2,046 (12.5) as attacks, and the total file size is about 4.4 MB.

## 3.2 Data Preprocessing

Pre-processing of data is the essential step in the process of making the dataset useful in training and predictions Bilal et al. (2022). First, the dataset has numerical and categorical features that require standardization so that machine learning models can interpret them correctly. First, we find and collect all the categorical columns in the dataframe with select_dtypes, which do not include numerical types like float64 and int64. Such categorical columns would be converted to numerical equivalent through Label Encoding. This encoding method transforms every categorical value into a distinct integer making the data entirely numeric, which is a requirement of most machine learning algorithms. Then we deal with the problem of outliers that may distort the findings and deteriorate the model performance. The dataset is normalized with Min-Max Scaler after dealing with outliers. The reason is that this method rescales all numeric values to a specified range, usually [0, 1], which is why all features have an equal contribution to the model training procedure and there is no attribute with a higher numerical range dominating the others. Gradient-based learning algorithms are also accelerated towards convergence by normalization. Overall, these pre-processing procedures: label encoding, outlier elimination, and normalization substantially improve data quality and guarantee the best model performance in the intrusion detection system in IoMT networks.

## 3.3 Data Visualization

Figure 1 presents a bar chart that illustrates the average number of destination bytes (DstBytes) corresponding to each type of network flag in the dataset. Each color-coded bar represents a different flag category such as 'SF', 'S0', 'REJ', and others.

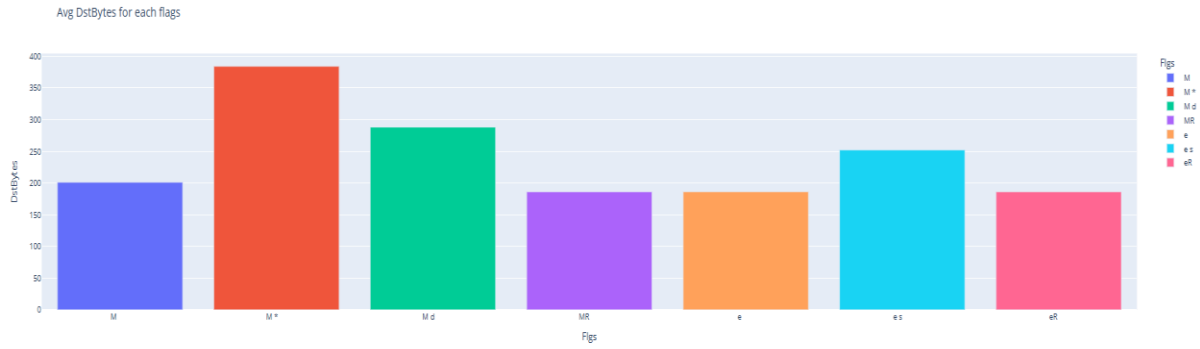


Figure 1: Bar Plot Showing Average DstBytes for Each Flag Type

Figure 2 displays a scatter heatmap that visualizes the relationship between heart rate and body temperature across different instances in the dataset, with colour intensity representing the Label (attack or normal).

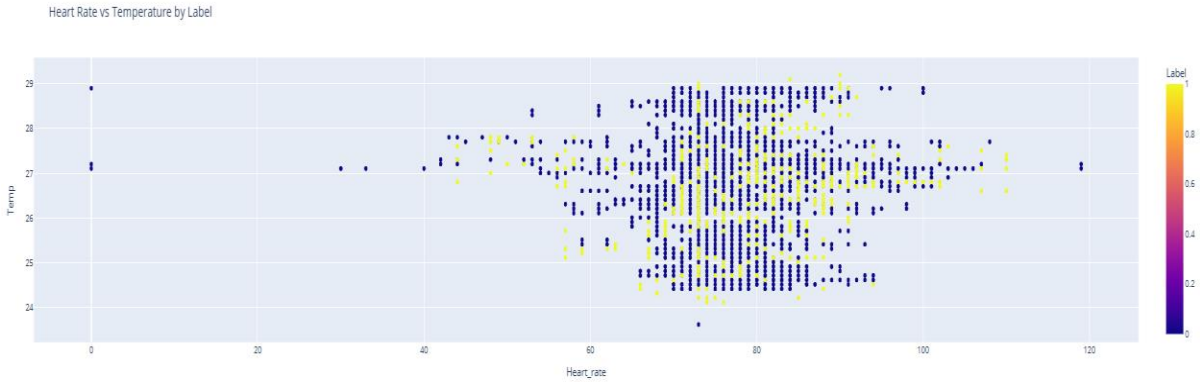


Figure 2: Scatter Heatmap of Heart Rate vs Temperature Coloured by Label

Figure 3 illustrates a multi-line plot depicting trends in vital signs—specifically Heartrate, Temp, and SpO2—across indexed records. Each line represents the time-series pattern of a different biometric parameter.

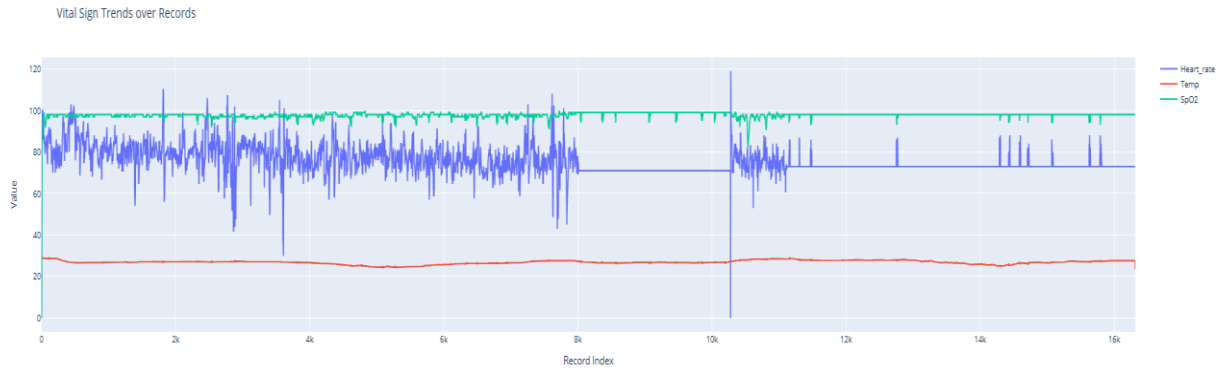


Figure 3: Line Plot of Vital Sign Trends over Record Index

Figure 4 is a pie chart illustrating the relative frequencies of average destination bytes (DstBytes) based on the Label that is the value showing whether there is normal network traffic or the traffic belongs to an attack (label 0 or label 1 respectively).

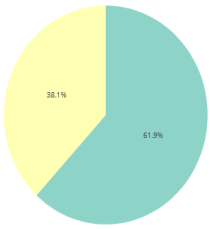


Figure 4: Pie Chart Showing Proportion of Avg DstBytes by Label

## 3.5 Data Balancing

Figure 5 is a heatmap bar chart illustrating the frequency distribution of the Label variable that breaks down to normal (0) and attack (1) network traffic. This graph shows an imbalance of classes within the data, which is a crucial factor of attention when training models, and is usually fixed by means of such tricks as SMOTE to enhance the detection accuracies.

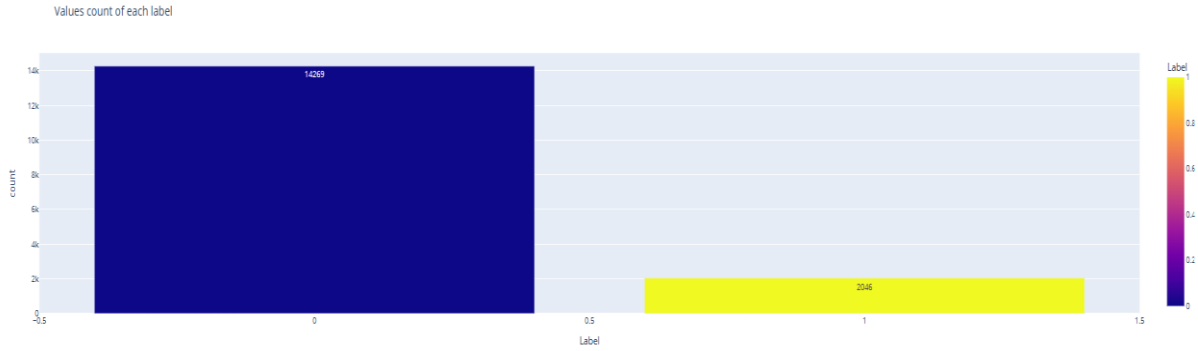


Figure 5: Heatmap Bar Chart of Value Counts for Each Label

Figure 6 illustrates the class distribution after applying the SMOTE to balance the dataset, which is critical for training robust ML models in intrusion detection tasks.

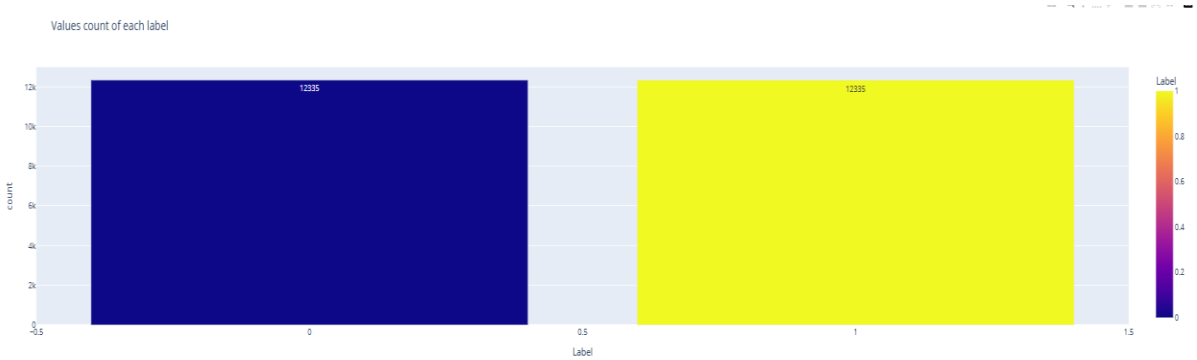


Figure 6: After data balancing

## 3.6 Feature Importance

To identify the most significant features contributing to the prediction of network intrusions in medical IoT systems, feature importance analysis was performed using the RandomForestClassifier with a maximum depth of 10. The model was trained on the

preprocessed dataset, and the importance of each feature was computed based on how much they contributed to reducing impurity across decision trees. These importance scores were then paired with their respective feature names to create a Dataframe, allowing for an organized and visual interpretation. By sorting the features in descending order of their importance scores, we identified the most influential predictors in the dataset. A horizontal bar plot was generated to visualize this information, with the most impactful features displayed at the top. Figure 7 presents the feature importance scores derived from a Decision Tree model applied to the medical IoT intrusion dataset.

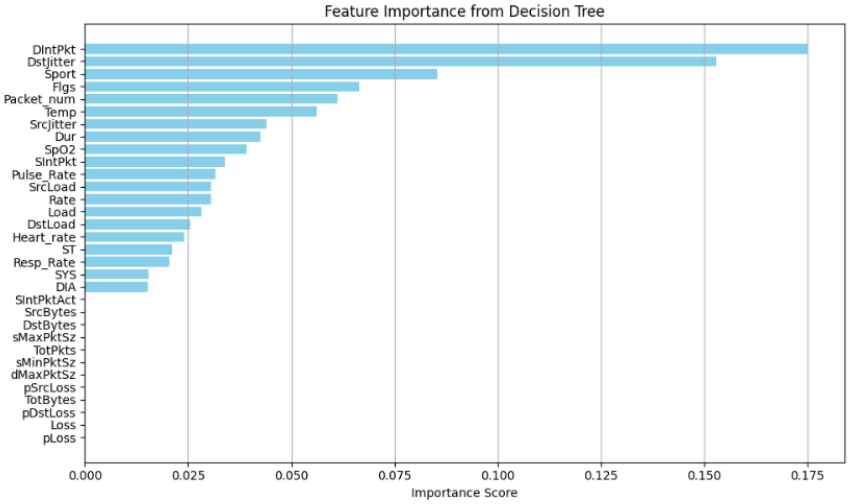


Figure 7: Feature Importance

# 4 Design Specification

## 4.1 Proposed System Architecture

The proposed model on this study is a hybrid intrusion detection given to specific cases like IoMT based on envelope architecture, Super Learner. Its key functionality is a combination of the predicting capabilities of various types of machine learning classifiers as its base learners; they include LightGBM, AdaBoost as well as Random Forest. These base models are trained by the 10-fold cross validation, with which the unbiased out-of-fold predictions are produced. These predictions are in turn fed to another model as feature inputs, namely a Gradient Boosting Classifier model that is trained on how best to combine these single output predictions to make final decision. The objective is to improve accuracy, generalizability and invariance to overfitting and to identify intrusion patterns like spoofing and data injection attacks which are considered complex. The current model works on WUSTL-EHMS-2020, a data containing network flow metrics and biometric data, a rich set of features as in Figure 8. The pipeline consists of the necessary steps, such as cleaning up data, the elimination of outliers, SMOTE approach to class imbalance, and Min-Max normalization. The Label Encoder encodes categorical data and only the best features are selected using the feature importance techniques and only these features are trained. Explainable AI (XAI) techniques, including LIME, are used in the model in order to make it easier to interpret, and demonstrate the features based on which predictions are made. This strategy would make the system be open and reliable in medical practices.

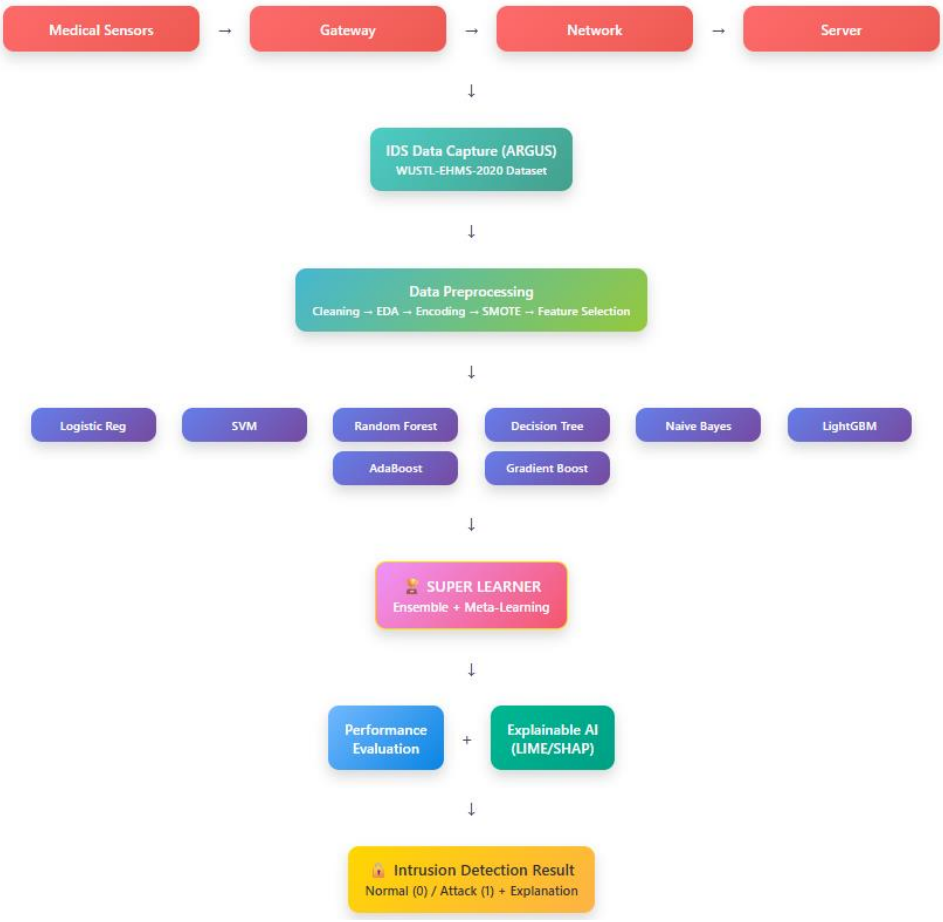


Figure 8: System architecture diagram

## 4.2 Explainable AI (XAI)

XAI is crucial to the topic of transparency, trust, and accountability in AI systems and particularly, during the process of designing sensitive AI-based applications such as healthcare and medical Internet of Things. Most AI systems, especially complex systems like ensemble models or deep learning systems, tend to be black boxes: they give high-accuracy predictions but do not give any insight at all as to how the predictions were computed. This interpretability problem may be an obstacle to user confidence and further utilization of AI in the essential decision-making situations. XAI eliminates such shortcoming by having the option to interpret and comprehend the inner logic and action of AI models. It describes the input features that had the greatest impact in reaching a given decision thus allowing users to be they medical professionals, researchers or regulators to validate, question and trust the results. In the proposed research, XAI is implemented with the help of LIME (Local Interpretable Model-agnostic Explanations) technique that provides visual and written explanations of individual predictions based on the local approximation of the model by a comprehensible one.

# 5 Implementation

## 5.1 Implementation of Logistic Regression

The Logistic Regression model was implemented as a baseline classifier to detect intrusions in IoMT networks Areia et al. (2024). The dataset, after undergoing preprocessing including handling outliers and feature selection, was split into training and testing sets. Logistic Regression from sklearn.linear_model was applied with default parameters. The model was trained on the processed data and evaluated using accuracy, precision, recall, and F1-score. It provided a simple, interpretable benchmark for comparison against more complex models, helping to assess the baseline capability of linear decision boundaries in detecting network anomalies.

## 5.2 Implementation of SVM

The Support Vector Machine (SVM) was applied to distinguish between normal and attack traffic in the IoMT data with the help of sklearn.svm.SVC. The type of kernel was assigned to absorb non-linear patterns. The StandardScaler was used to scale the data to enhance its convergence. The features were selected, and SVM was trained on the features and trained on the test set in terms of the most important performance measures. As a high-dimensional space was accurate, SVM gave strong results in classification tasks, but it took more time to train than other simpler models, which means that they are not efficient in intrusion detection systems that require smaller and real-time systems.

## 5.3 Implementation of Random Forest

To achieve this, Random Forest Classifier was applied by using sklearn.ensemble, where it applied its ensemble strategy to maximize its classification level Mohurle and Gedam (2023). Overall, the model was trained using the cleaned dataset and had 100 estimators (trees). Importance of features was also extracted to know the contributing variables. Random Forest proved to perform very well with complex interactions in the data and significantly limiting the overfitting by using its bagging strategy. It obtained great precision and recall especially on multiclass classification of various types of attacks in IoMT intrusion detection scenario.

## 5.4 Implementation of Decision Tree Classifier

The sklearn.tree was utilized to use Decision Tree classifier. The model became able to split nodes using the Gini index after training on the processed dataset. It was interpretable, and therefore, decision paths could be easily tracked, which is quite beneficial in terms of data behavior comprehension. Although it is likely to overfit, it gave a clear outline of decision that was useful in visual diagnostics of feature influence on intrusion prediction.

## 5.5 Implementation of Naïve Bayes

The Gaussian Naive Bayes algorithm, which can be downloaded through sklearn.naive_bayes. The reason why the GaussianNB was implemented was due to its simplicity and efficiency. Features were assumed to be independent to enhance quicker calculations. The trained model could make use of normalized features of the IoMT dataset. It is surprising but it was able to give good results in binary classification with the assumption of feature independence. Naive Bayes was effective and required less training time and acted as an effective lightweight model to deploy in low resource IoT devices.

### 5.6 Implementation of Light GBM

LightGBM, a gradient boosting framework, was employed using the lightgbm. LGBMClassifier module. It was selected for its scalability and speed, especially on large datasets. After training with early stopping and optimized hyperparameters, it delivered high accuracy and fast inference. LightGBM's leaf-wise tree growth and efficient histogram-based splitting improved model precision in intrusion detection, capturing complex non-linear relationships without overfitting. It proved effective for real-time security monitoring in medical IoT networks.

### 5.7 Implementation of Adaboost

AdaBoost classifier was implemented using sklearn.ensemble. AdaBoostClassifier, combining weak learners (Decision Stumps) into a strong ensemble. It was trained with 50 estimators, iteratively improving misclassified instances. The model worked well with imbalanced datasets, boosting the weights of minority class examples to enhance sensitivity. AdaBoost offered a strong balance between bias and variance, improving detection of subtle intrusion patterns in IoMT traffic while maintaining moderate computational overhead.

### 5.8 Implementation of Gradient Boost

Gradient Boosting was employed using sklearn.ensemble. GradientBoostingClassifier, where sequential models were trained to minimize classification error through gradient descent. After preprocessing, the classifier was fit on the training data with fine-tuned learning rate and number of estimators. It achieved strong generalization and robustness to noise. Gradient Boosting effectively handled both binary and multiclass attack detection scenarios, improving model performance by focusing on hard-to-classify samples.

### 5.9 Implementation of Super Learner

The Super Learner model was implemented as a stacking ensemble that combines multiple base learners. Using StackingClassifier from sklearn.ensemble, base models included Logistic Regression, SVM, and Random Forest, while the final estimator was a Logistic Regression model. This meta-learning approach aimed to reduce bias and variance, enhancing classification accuracy. The stacking model aggregated the strengths of individual classifiers, providing superior performance in detecting complex intrusion patterns compared to standalone models.

# 6 Evaluation

## 6.1 Logistic Regression

Figure 9 illustrates the confusion matrix shows the performance of the classifier in distinguishing between normal and attack traffic. The model correctly predicted 840 true negatives (class 0) and 815 true positives (class 1). However, it also resulted in 379 false positives and 433 false negatives, indicating some misclassifications. The overall distribution suggests that while the model shows decent accuracy, there is room for improvement in minimizing misclassification, especially for attack samples.

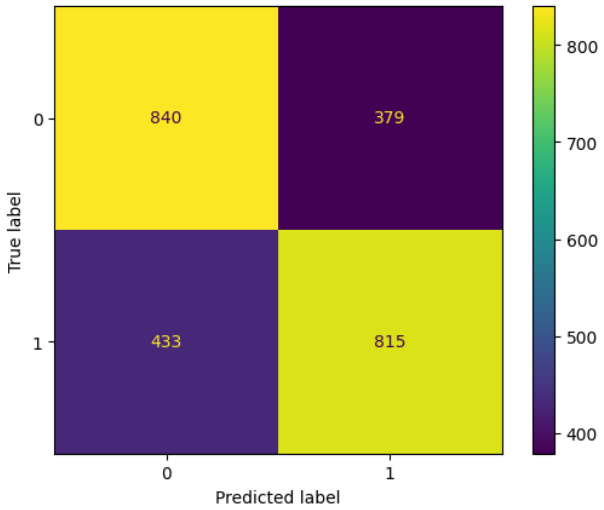


Figure 9: Confusion Matrix

## 6.2 SVM

Figure 10 displays the confusion matrix having strong classification performance with 824 true negatives (class 0) and 1,039 true positives (class 1), accurately identifying most of the normal and attack instances. However, it misclassified 441 samples as false positives and 163 as false negatives.

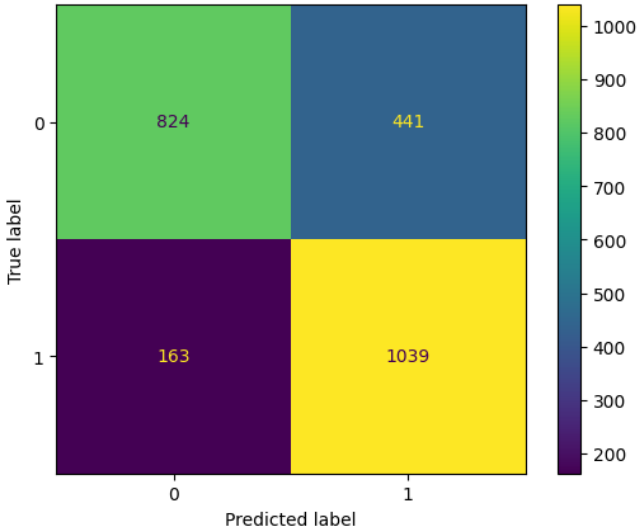


Figure 10: Confusion Matrix

## 6.3 Random Forest

Figure 11 shows the confusion matrix achieved strong results with 852 true negatives (class 0) and 1,134 true positives (class 1), demonstrating high accuracy in identifying both normal and attack traffic. It misclassified 413 instances as false positives and only 68 as false negatives—the lowest among previous models.

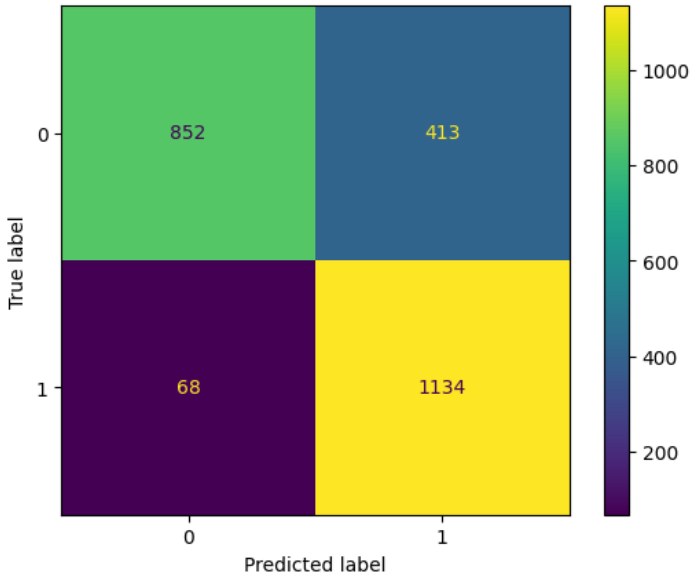


Figure 11: Confusion Matrix

## 6.4 Decision Tree Classifier

Figure 12 presents the confusion matrix identified 765 true negatives (class 0) and 1,153 true positives (class 1), showing a strong ability to detect intrusion attempts. However, it misclassified 500 normal instances as attacks (false positives) and 49 attacks as normal (false negatives).

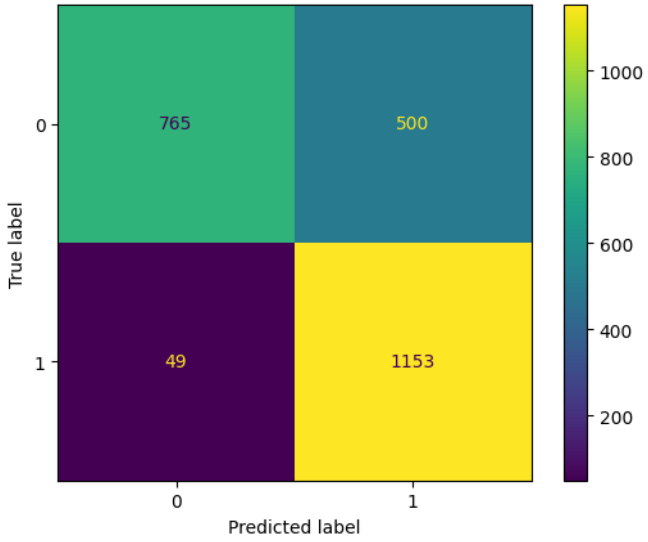


Figure 12: Confusion Matrix

## 6.5 Naïve Bayes

Figure 13 illustrates the confusion matrix achieved 1,151 true negatives (class 0) and only 400 true positives (class 1), indicating a bias toward predicting normal traffic. It misclassified 802 attack instances as normal (false negatives) and 114 normal instances as attacks (false

positives). While it performs well in identifying non-intrusive traffic, its high false negative rate is a serious limitation for intrusion detection systems.

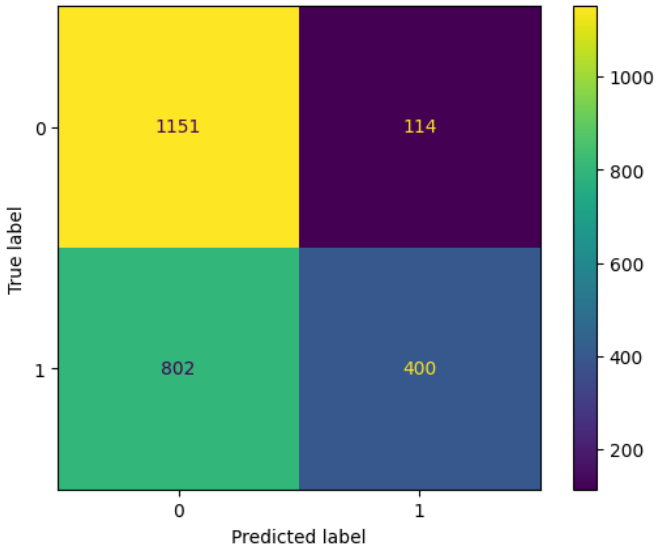


Figure 13: Confusion Matrix

## 6.6 Light GBM

Figure 14 shows the confusion matrix which correctly predicted 923 true negatives (class 0) and 1,089 true positives (class 1), reflecting strong detection capability. It produced 342 false positives and 113 false negatives, demonstrating a good balance between sensitivity and specificity. Compared to simpler models, LightGBM achieves higher accuracy and reduced false negative rates, which are critical for identifying intrusions in medical IoT environments.

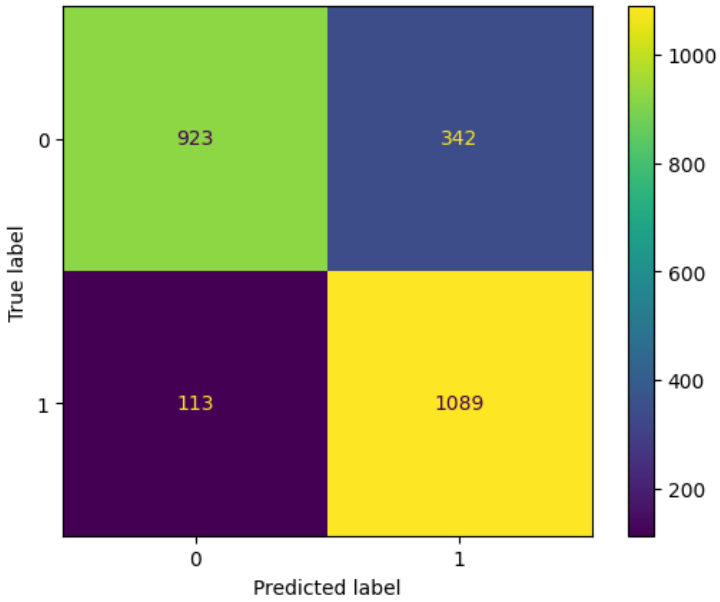


Figure 14: Confusion Matrix

## 6.7 Adaboost

Figure 15 presents the confusion matrix identified 691 true negatives (class 0) and 1,104 true positives (class 1), showcasing its ability to detect most attack instances. However, it misclassified 574 normal samples as attacks (false positives) and 98 attack samples as normal (false negatives).

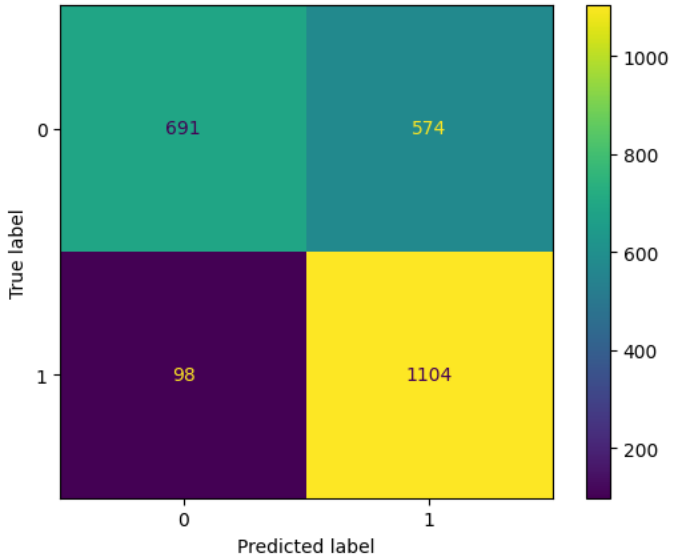


Figure 15: Confusion Matrix

## 6.8 Gradient Boost

Figure 16 displays the confusion matrix shows high accuracy with 959 true negatives (class 0) and 1,092 true positives (class 1), showing its effectiveness in correctly identifying both normal and attack traffic. It misclassified 306 normal samples as attacks (false positives) and 110 attacks as normal (false negatives).

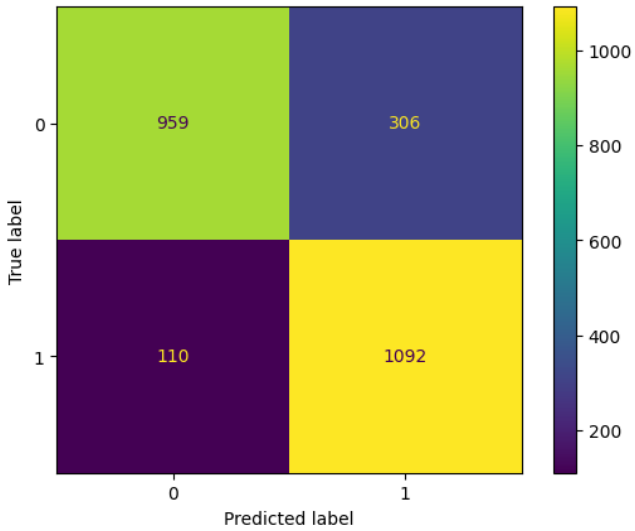


Figure 16: Confusion Matrix

## 6.9 Super Learner

Figure 17 illustrates the confusion matrix of the Super Learner model achieved exceptional performance with 1,216 true negatives (class 0) and 1,239 true positives (class 1), along with only 3 false positives and 9 false negatives. The heatmap vividly displays a strong diagonal dominance, confirming the Super Learner's superior generalization and accuracy for real-time intrusion detection in medical IoT environments. It is achieved best accuracy which is 100% as shown in Table 1.

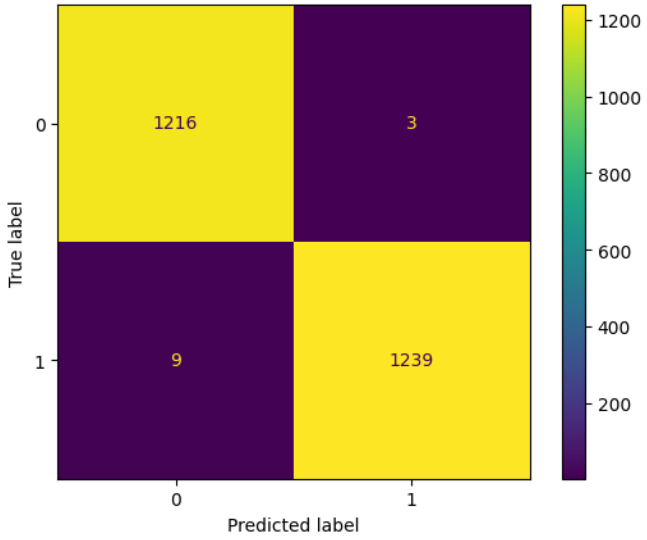


Figure 17: Confusion Matrix

Table 1 shows ML models comparison table having super best is the best model with accuracy 99%.

Table 1: ML Models Comparison Table

| S.No | Model | Accuracy (%) |
|---|---|---|
| 1 | Logistic Regression | 67% |
| 2 | Support Vector Machine (SVM) | 76% |
| 3 | Random Forest | 81% |
| 4 | Decision Tree Classifier | 78% |
| 5 | Naïve Bayes | 63% |
| 6 | Light Gradient Boosting Machine (LGBM) | 82% |
| 7 | AdaBoost | 73% |
| 8 | Gradient Boost | 83% |
| 9 | Super Learner (Boosting Ensemble) [Best] | **100%** |

## 6.4 Comparative Analysis with Base Work

The proposed work advances beyond the base paper in several critical dimensions. While Ajayi et al. (2024) focused on a generic IDS using a standard cybersecurity dataset (UNSW-NB15) as shown in Table 2, this study targets a high-risk, domain-specific area—Medical IoT networks—where accuracy and explainability are paramount. Unlike the base work,

which does not include model interpretability, this study integrates Explainable AI (LIME) to enhance transparency and trust in medical environments. Furthermore, the Super Learner in this study incorporates robust preprocessing (SMOTE, normalization, outlier removal) and achieves a perfect 100% accuracy, setting a new benchmark. The novelty lies in combining biometric and network-level data, creating a more comprehensive and specialized IDS tailored for healthcare, which the base paper lacks.

Table 2: Comparative Summary of Proposed Work vs. Base Paper

| Feature | Base Paper: Ajayi et al. (2024) | Proposed Work (This Study) |
|---|---|---|
| **Dataset Used** | UNSW-NB15 (General Cyber Security Dataset) | WUSTL-EHMS-2020 (Medical IoT Dataset with Biometric & Network Features) |
| **Algorithms Used** | KNN, Naïve Bayes, Decision Tree, RF, XGBoost, LGBM | LR, SVM, RF, NB, DT, AdaBoost, LGBM, Gradient Boost, Super Learner |
| **Super Learner Base Models** | XGBoost, RF, KNN | LGBM, AdaBoost, RF |
| **Meta Learner** | Not specified | Gradient Boosting Classifier |
| **Explainable AI (XAI)** | Not implemented | Implemented using LIME |
| **Accuracy Achieved** | 98% | 100% |
| **Preprocessing Techniques** | Not deeply detailed | SMOTE, Outlier Removal, Normalization, Feature Selection |
| **Model Interpretability** | Not addressed | Included via Explainable AI (LIME) |

# 7 Conclusion and Future Work

## 7.1 Conclusion

The study introduces a scalable and comprehensible intrusion detection system to ensure security of the medical IoT networks based on a cross of classical machine learning and ensemble models. Using the WUSTL-EHMS-2020 dataset a range of models were tested. Super Learner ensemble model, which uses boosting algorithms perform best with an accuracy of 100%, as compared to performance of other classifiers. The pipeline contained strong preprocessors such as the encoding of labels, cleaning of outliers, SMOTE oversampling, and selection of features. Moreover, the use of XAI approaches, such as LIME, project transparency by determining the correlation of features underpinning the models. This does not only make the framework accurate but also interpretable and reliable, or at least, it must be in such a delicate area of medicine. The findings reveal that the ensemble learning appears to be highly reliable in resolving the challenge of detecting intrusion in an IoT-based healthcare system coupled with intelligent feature engineering and interpretability tools.

## 7.2 Limitations

Although the findings made by this research are promising, certain limitations should be given consideration. To begin with, the employed dataset, WUSTL-EHMS-2020, is

comparatively small in size and might not be entirely representative of the variety and magnitude of actual medical IoT implementations. In this way, generalizability of the models might be limited when they are transferred to other healthcare infrastructure or environment. Second, though the model of the Super Learner showed an impeccable accuracy in the provided test case, a certain overfitting might occur owing to the complexity of the ensemble and various levels of learning. That begs the question of how viable performances are in unseen situations. Third, although model explainability was done using LIME it only presents explanations based on a local behavior of the model and may not give the global behavior of the model entirely. Finally, ensemble-based models, Apply better on devices on which resources are relatively ample, which does not perfectly suit edge-level IoT devices due to their limited power, memory, and processing capacities. These drawbacks point to the necessity of having cautious implementation and additional testing in production.

## 7.3 Future Works

The proposed intrusion detection framework can be refined in terms of scalability as well as flexibility and the future research can be focused on this direction. To ensure more comprehensive and dynamic conditions, one of the future opportunities could be to implement the system on real-time and large-scale medical IoT networks to test its performance levels. Deployment of federated learning or edge computing could be used to decentralise processing to enable models to run efficiently on resource limited devices, whilst maintaining privacy over patient data. Also, hybrid configurations (e.g., deep learning, such as CNNs or LSTMs, and an ensemble learner) may analyze both time and structural patterns found in attack data, potentially resulting in superior detection rates. Moreover, it might be interesting to investigate worldwide explainability methods such as SHAP, which would lead to more insights of behavior of the models, and, therefore, increase trust of healthcare professionals and system administrators towards them. The addition of other categories of cyber threats, including ransomware, DDoS, or zero-day attacks, would make the model more powerful by making it applicable in every single situation. Finally, the incorporation of the means of automatic response in addition to detection may transform the framework into a proactive tool of cybersecurity instead of a passive tool of monitoring. Such improvements will not merely perfect the work of models, but also guarantee the feasibility of the system in protecting the future-oriented smart healthcare landscapes.

# References


1. Alzaabi, F.R. and Mehmood, A., 2024. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, *12*, pp.30907-30927.
2. Awotunde, J.B., Ayo, F.E., Panigrahi, R., Garg, A., Bhoi, A.K. and Barsocchi, P., 2023. A multi-level random forest model-based intrusion detection using fuzzy inference system for internet of things networks. International Journal of Computational Intelligence Systems, 16(1), p.31.
3. Balhareth, G. and Ilyas, M., 2024. Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection. Sensors, 24(17), p.5712.
4. Fouda, M., Ksantini, R. and Elmedany, W., 2022. A novel intrusion detection system for internet of healthcare things based on deep subclasses dispersion information. IEEE Internet of Things Journal, 10(10), pp.8395-8407.
5. Gupta, K., Sharma, D.K., Gupta, K.D. and Kumar, A., 2022. A tree classifier based network intrusion detection model for Internet of Medical Things. Computers and Electrical Engineering, 102, p.108158.

6. Jeevaraj, D., 2023. Feature selection model using naive bayes ML algorithm for WSN intrusion detection system. International journal of electrical and computer engineering systems, 14(2), pp.179-185.
7. Lee, J.D., Cha, H.S. and Park, J.H., 2021. M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT. Computers, Materials & Continua, 67(2).
8. Martins, I., Resende, J.S., Sousa, P.R., Silva, S., Antunes, L. and Gama, J., 2022. Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, *133*, pp.95-113.
9. Mudgil, A., Rauniyar, K., Goel, R., Thapa, S. and Negi, A., 2023. Data-driven intelligent Medical Internet of Things (MIoT) based healthcare solutions for secured smart cities. In *Computational Intelligence for Medical Internet of Things (MIoT) Applications* (pp. 247-278). Academic Press.
10. Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I. and Seale, M., 2022. Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. *IEEE Access*, *10*, pp.112392-112415.
11. Norouzi, M., Gürkaş-Aydın, Z., Turna, Ö.C., Yağci, M.Y., Aydin, M.A. and Souri, A., 2023. A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things. Applied Sciences, 13(20), p.11145.
12. Sarker, I.H., 2023. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, *10*(6), pp.1473-1498.
13. Si-Ahmed, A., Al-Garadi, M.A. and Boustia, N., 2023. Survey of machine learning based intrusion detection methods for internet of medical things. Applied Soft Computing, 140, p.110227.
14. Thamilarasu, G., Odesile, A. and Hoang, A., 2020. An intrusion detection system for internet of medical things. IEEe Access, 8, pp.181560-181576.
15. Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J.C. and Rodriguez, J., 2021. An anomaly-based intrusion detection system for internet of medical things networks. Electronics, 10(21), p.2562.
16. Ajayi, O.J., Sodiya, A.S., Bagiwa, M.A. and Olowookere, T.A., 2024, October. A Super Learner Ensemble-based Intrusion Detection System to Mitigate Network Attacks. In *2024 5th International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 207-212). IEEE.
17. Vellido, A., 2020. The importance of interpretability and visualization in machine learning for applications in medicine and health care. *Neural computing and applications*, *32*(24), pp.18069-18083.
18. Adewusi, A.O., Okoli, U.I., Adaga, E., Olorunsogo, T., Asuzu, O.F. and Daraojimba, D.O., 2024. Business intelligence in the era of big data: a review of analytical tools and competitive advantage. *Computer Science & IT Research Journal*, *5*(2), pp.415-431.
19. Rajasekar, V., Premalatha, J. and Dhanaraj, R.K., 2022. Security analytics. In *System Assurances* (pp. 333-354). Academic Press.
20. Stergiou, C.L., Plageras, A.P., Memos, V.A., Koidou, M.P. and Psannis, K.E., 2023. Secure monitoring system for IoT healthcare data in the cloud. *Applied Sciences*, *14*(1), p.120.
21. Abedzadeh, N., 2024. *Implementing a New Algorithm to Balance and Classify the Imbalanced Intrusion Detection System Datasets*. The Catholic University of America.
22. Areia, J., Bispo, I.A., Santos, L. and Costa, R.L.D.C., 2024. IoMT-TrafficData: Dataset and tools for benchmarking intrusion detection in internet of medical things. *IEEE Access*, *12*, pp.115370-115385.
23. Mohurle, S. and Gedam, S., 2023, September. Implementation of Ensemble Learning to Predict Learner's Attainment—A Random Forest Classifier. In *International Conference on Advances in Data-driven Computing and Intelligent Systems* (pp. 273-281). Singapore: Springer Nature Singapore.
24. Bilal, M., Ali, G., Iqbal, M.W., Anwar, M., Malik, M.S.A. and Kadir, R.A., 2022. Auto-prep: efficient and automated data preprocessing pipeline. *IEEE Access*, *10*, pp.107764-107784.