
Journal of Informatics and Web Engineering

Vol. 3 No. 3 (October 2024)

eISSN: 2821-370X

Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker

Suliat Toyosi Jimoh¹, Shaymaa S Al-juboori^{2*}

^{1,2}School of Computing, Engineering and Mathematics, University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom

*Corresponding author: (shaymaa.al-juboori@plymouth.ac.uk; ORCID: 0000-0001-5175-736X)

Abstract - This study aims to enhance the cybersecurity framework of pacemaker devices by identifying vulnerabilities and recommending effective strategies. The objectives are to pinpoint cybersecurity weaknesses, utilize machine learning to predict security breaches, and propose countermeasures based on analytical trends. The literature review highlights the transformation of pacemaker technology from basic, fixed-rate devices to sophisticated systems with wireless capabilities, which, while improving patient care, also introduce significant cybersecurity risks. These risks include unauthorized entry, data breaches, and life-threatening device malfunctions. The methodology in this study utilizes a quantitative research approach using the WUSTL-EHMS-2020 dataset, which includes network traffic features, patients' biometric features, and attack label. The step-by-step method of machine learning prediction includes data collection, data preprocessing, feature engineering, and models' training using Support Vector Machines (SVM) and Gradient Boosting Machines (GBM). The implementation results used evaluation metrics like accuracy, precision, recall, and F1 score to show that GBM model outperformed the SVM model. The GBM model achieved higher accuracy of 95.1% compared to 92.5% for SVM, greater precision of 99.6% compared to 96.7% for SVM, better recall of 94.9% compared to 42.7% for SVM, and a higher F1 score of 76.3% compared to 59.0% for SVM, making GBM model more effective in predicting cybersecurity threats. This study concludes that GBM is an effective machine learning model for enhancing pacemaker cybersecurity by analyzing network traffic and biometric data patterns. Future recommendations for improving the pacemaker cybersecurity include implementing GBM model for threat predictions, integration with existing security measures, and regular model updates and retraining.

Keywords— Cybersecurity, Pacemaker, Vulnerabilities, Machine Learning, Threat Prediction.

Received: 10 July 2024; Accepted: 30 August 2024; Published: 16 October 2024

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

The rapid development of technology has transformed how medical procedures are performed, especially through the integration of advanced electronic devices [1], [2], [3]. As mentioned in [4], a significant development in modern medicine is the widespread use of medical implantable devices like pacemakers. These pacemakers, which are designed to regulate heart rhythms, have improved patients' lives and overall wellbeing. The essential features that make pacemakers revolutionary are their ability to communicate wirelessly with healthcare providers, and adjust to patients needs through remote monitoring, which also introduces a variety of vulnerabilities. The global landscape of

threats has undergone significant transformation alongside the rapid evolution of a digitally interconnected society. Medical devices, once seen purely in the light of their therapeutic potentials, are now viewed through the lens of cybersecurity [6]. With the advent of IoT (Internet of Things), home appliances and medical equipment are now interconnected in ways that were not previously adopted, enabling streamlined operations and remote access functionalities [1]. However, this interconnectivity has increased the attack surface for potential adversaries [5], [7] [8].

The above-mentioned points have evidenced the importance of ensuring pacemaker cybersecurity. In regular security breaches, the primary concern is usually financial or information loss, however, security breaches or vulnerabilities in pacemakers can be a threat to patients' lives [9], [7], [10]. For example, a pacemaker's release of electric shock to a patient may lead to death [11], [10]. Researchers and cybersecurity professionals have detailed how these medical devices could be manipulated or disrupted by cyber-attackers. According to [12], [13], [14], [15], cyber-attackers could potentially endanger patients' lives by remotely manipulating or disabling pacemaker settings through vulnerabilities in the device's telemetry functions. The integration of technology into medical science has transformed the healthcare system's regulatory and ethical framework, often causing delay between advancements in technology and the establishment of comprehensive governance measures [2].

The cyber risks associated with pacemakers are not just technical in nature, but also have societal implications as well [16]. Patients' knowledge of potential pacemaker vulnerabilities can induce anxiety, thereby affecting their overall trust in medical interventions. For example, when U.S. Vice President Dick Cheney in 2013 disabled his pacemaker's wireless features due to fears of being hacked [17]. Healthcare providers face the challenge of ensuring device functionality while also ensuring cybersecurity. [18] shows that adding layers of security might impede the timely delivery of critical care in emergencies.

The fundamental problem in modern pacemaker devices is that, while they improve healthcare management through remote wireless functionalities, they also expose patients to cyber risks such as unauthorized access and potential pacemaker manipulation, thereby causing threats to both patients' safety and data privacy. The aim of this study is to strengthen pacemaker device cybersecurity by identifying potential vulnerabilities and recommending effective strategies. The objectives of the study are to identify pacemaker systems cybersecurity vulnerabilities from related research, use machine learning to predict potential security breaches by analyzing cyber trends and patterns, and recommend effective countermeasures.

The contributions of this study are summarized as follows:

1. Identifying pacemaker device vulnerabilities.
2. Using SVM and GBM machine learning models to predict potential security breaches in pacemaker devices. And demonstrating the performance of GBM and SVM models using evaluation metrics like accuracy, precision, recall, and F1 score.
3. Utilized the WUSTL-EHMS-2020 dataset that includes network traffic features and biometric data, to facilitate the prediction of potential security breaches.
4. Recommendations of future strategies like implementing the GBM model for threat prediction, integrating machine learning with existing security measures, regular model updates and retraining, compliance with regulations, improving user awareness & training, conducting regular risk assessments & audits, and effective incidence response approach.

The rest of the paper is organized as follows. Section 2 describes the literature review in detail, covering existing techniques and methods used for text summarization. Section 3 proposes the methodology; covering the dataset description and the overall approaches used, and the implementation of the proposed solution has also been discussed. Section 4 presents quantitative and qualitative analysis and discusses the results in detail compared to previous approaches. Section 5 presents concluding remarks on the overall research work and points out the future research directions.

2. LITERATURE REVIEW

Rapid improvements in medical technology have made it possible to integrate complex electronic devices into healthcare systems, which has improved patient outcomes [3]. Among these medical advancements, implanted cardiac

devices, like pacemakers, are essential for controlling cardiac arrhythmias since they stimulate the heart with electrical impulses to keep its heart rate appropriate. Heart care has changed dramatically because of pacemakers' development from basic, fixed-rate devices to sophisticated systems that can modify pacing in real-time based on the needs of the heart and communicate wirelessly for configuration and monitoring [21].

2.1 Pacemaker Overview

A pacemaker as shown in Figure 1 is a cardiac implantable medical device that regulates abnormal heart by sending electrical impulses to stimulate the heart when it is beating too slowly or irregularly [5], [22], [10]. Pacemakers have evolved significantly over the years, transitioning from simple devices that deliver fixed-rate pacing without sensing to sophisticated systems capable of sensing the heart's electrical activity and adjusting pacing accordingly. Modern pacemakers are also capable of communicating wirelessly with external devices for monitoring and configuration, enhancing both patient care and convenience [23].



Figure 1. A Medical Pacemaker [24]

The pacemaker ecosystem is an interconnected system that relies on the seamless integration of multiple components, including the devices, the stake holders (patients, doctors & manufacturers) and their interactions [25]. Each component plays an essential role to ensure effective and secure operation of the pacemaker, contributing to the maintenance of patient's cardiac health and protection of sensitive health information. Data transmission within the pacemaker ecosystem involves several key interactions essential for effective patient care management as described by [25]. The data on patient's heart activity and device functionality is first transmitted from the pacemaker to external programmers that healthcare providers use. This data is then often uploaded from the programmers to electronic health record systems within healthcare facilities, allowing for integrated patient management. In more advanced setups, data can be transmitted directly from pacemakers to remote monitoring systems as described by [26], enabling continuous care management, and reducing the need for frequent hospital visits. This flow of data ensures that patient health is monitored and managed in real-time, thereby boosting the effectiveness and responsiveness of health services.

The wireless connectivity of the pacemaker as part of the IoMT architecture, is also discussed to have an insight into the pacemaker technology and how patients' cardiac data are transmitted and processed. This IoMT architecture illustrated in Figure 2 consists of the perception, network, and application layers. The perception layer, which is the fundamental layer, consists of the pacemaker device itself, which acts as the primary sensor, equipped with the necessary hardware to monitor the patient's heart rate, rhythm, and other vital parameters [8], [21], [27]. The perception layer collects and transmits the data to the next layer using communication protocols such as Bluetooth, NFC, ZigBee, Wi-fi, and so on. [21], [27]. The network layer enables the transmission of data collected by the pacemaker to the application layer. This layer utilizes short-range protocols like BLE and Zigbee, for communication between the pacemaker and a nearby gateway device (e.g., smartphone or dedicated receiver), and long-range communication (cellular networks, e.g., 5G, 4G, LPWAN) for transmitting data from the gateway device to remote servers or the cloud [28], [21], [27]. The application layer, as discussed by [28], [8], [21], [27], processes, and analyzes the data received from the pacemaker, providing services to healthcare professionals and patients. The application layer includes cloud-based servers for data storage and processing [28], Electronic Health Record (EHR) systems for integrating pacemaker data with the patient's medical history [27], user interfaces for healthcare professionals to

monitor and manage patient data [8], and mobile applications for patients to access their pacemaker data and communicate with healthcare providers.



Figure 2. The IoMT Architecture [21]

2.2 Identified Pacemaker Cybersecurity Vulnerabilities

Pacemaker devices are vulnerable to several factors that could potentially compromise patient safety and privacy, which includes the integration of wireless capabilities, the lack of comprehensive security measures, and the limitations of the embedded systems. The presence of wireless capabilities enables remote monitoring and adjustment of the pacemakers [19], [21], [30], which also introduce new attack surfaces that were not present in older pacemaker models. This vulnerability could allow attackers to reprogram the pacemaker, deplete its battery life, or even induce shock into patients' hearts, thereby causing severe risks to the patients' well-being. Another significant vulnerability stems from inadequate encryption and robust authentication mechanisms in the communication channel between the pacemaker and external devices. [31], [14], [19], [32], discussed that many existing implantable devices do not employ strong encryption, making them easy targets for eavesdropping to easily intercept sensitive patient information, such as medical history and device settings and attacks which could compromise patient safety. This also introduces vulnerability that could be exploited by cyber-attackers. In the year 2010, the U.S. Food and Drug Administration (FDA) issued a recall for 23 cardiac pacemakers that were found to be defective and at least six of these recalled pacemakers had defects that were specifically attributed to flaws or errors in their software components [33]. Regulatory agencies such as the FDA have issued security recommendations and guidance for medical devices, these are largely non-binding and do not establish legally enforceable responsibilities [34], [35], [36]. [36], discussed that the absence of firm mandates allows manufacturers to make their own decisions regarding cybersecurity based on factors like cost and time-to-market rather than being compelled to adhere to strict security standards. Similarly, healthcare organizations struggling with limited resources may choose not to follow the regulatory guidelines if implementing the necessary security measures requires additional expenditures or diverts resources from other priorities. These regulatory gaps can lead to severe incidents like the 2017 recall of 465,000 pacemakers by FDA caused by vulnerabilities [36].

2.3 Pacemaker Cyber-attacks

Pacemakers are vulnerable to several cyber-attacks that threaten their security and functionality, like eavesdropping attacks, which involve unauthorized interception of data [37], [21], [30]. A Man-in-the-Middle (MITM) attack involves intercepting and potentially altering communications between the device and its controller [37], [21], [10]. Also, the control parameter attack, where cyber-attackers alter the device's settings to harmful values [10]. The real-world incidences of pacemaker attacks highlight the severity of cybersecurity threats to these critical medical devices. For example, in 2013, the former U.S. Vice President Dick Cheney disabled his pacemaker's wireless features, due to fears of hacking and assassination attempts [38], [39], [17]. Also, in 2015, the US FDA recalled 465,000 St. Jude

pacemakers after identifying cybersecurity risks that might impact the devices [7], [13]. These incidents highlight the necessity for strong cybersecurity defenses to maintain patients' 'safety and pacemakers' performance. The pacemaker vulnerabilities as mentioned above can have severe consequences like device malfunctions, rapid battery depletion, or inappropriate pacing, causing medical emergencies and heightened patient anxiety [25]. For healthcare providers, addressing these vulnerabilities requires expensive approaches like device recalls, replacement surgeries, and extended hospital stays to manage complications [40]. For instance, major occurrences like the NHS WannaCry show the impact of cyber-attacks on healthcare systems, which can lead to canceled appointments, surgical delays, and operational disruptions and indirectly affect patient care [40].

2.4 The need for Machine Learning

Machine learning is an effective mitigation approach that offers several key benefits. Firstly, it can create adaptive and intelligent security systems by learning from data and continuously enhancing their performance [41], [42]. Through training on normal device network behavior patterns, machine learning algorithms provide real-time monitoring capabilities, enabling quick detection of anomalies that may signal potential cyber-attacks, and response to these attacks [41], [15]. Secondly, machine learning enables the development of predictive security measures and customized security protocols tailored to individual device needs and threat profiles [17]. In the context of pacemakers, where prompt detection and mitigation of threats can be lifesaving, this real-time monitoring is of utmost importance. To strengthen the cybersecurity framework of medical pacemakers, machine learning will be used to predict potential security breaches on the pacemaker device network by analyzing cyber trends and patterns on the network. Table 1 below summarizes different related work that adopt machine learning in the medical domain.

Table 1. Analysis of Related Work

Literature Title	Author/year	Method used	Findings	Limitations
Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System	Zubair, et al., 2022 [43]	Deep Learning based IDS using DNN and ML models (LR, DT, SVM, RF, NB, IF, KM, LOF).	Achieved 99% accuracy	Dataset has class imbalance; model deployment and overhead not evaluated.
A Particle Swarm Optimization and DL for Intrusion Detection System IoT	Chaganti, et al., 2022 [44]	PSO-DNN based IDS using Machine Learning models such as LR, KNN, DT, AdaBoost, RF, & SVM, and DL	PSO-DNN achieved 96% accuracy, outperforming other ML and DL models.	Dataset lacks certain attack types like DoS; adversarial attacks not considered.
A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks.	Fang, et al., 2021 [45]	Detecting Illegal Behavior (DIB) using RST, SVM and R-FCVM.	R-FCVM achieved 92.67% average accuracy in identifying abnormal device behavior	Dataset does not fully represent the real-world cyber-attacks on IoMT. There is limited evaluation of the computation cost.
An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks	Zachos, et al., 2021 [46]	Hybrid anomaly-based IDS utilizing host and network techniques such as SVM, KNN, RF, LR, NB, and DT.	Most suitable algorithms for the detection components are DT, RF, and KNN. High detection accuracy for both datasets.	There is a need for balancing computational cost and detection efficiency.

An Intrusion Detection System for Internet of Medical Things	Thamilarasu, et al., 2020 [47]	Mobile Agent Based IDS using SVM, DT, NBC, KNN, RF ML for network level intrusion detection and Polynomial Regression Algorithm.	99.6% accuracy for network level and 98.2% accuracy for device level intrusion detection against malicious attacks. Low energy overhead of 5-7%.	The proposed system requires substantial computational resources for processing real-time intrusion detection. The setup is simulation and not real IoMT devices.
Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study	Hady, et al., 2020 [48]	RF, KNN, SVM, and ANN models applied on combined network and biometric data.	Combining network flow metrics with biometric data improves the performance of the proposed system with AUC ranging from 7% to 25%.	The proposed system's performance is not at its most efficient, research is needed to improve techniques, minimize feature space, and use more advanced attacks.

Based on Table 1, the SVM model was used across all the literature in the attached files, demonstrating its broad application and effectiveness in predicting cyber threats in the medical domain. The authors [45], [46], used the DIB system and the Anomaly-based IDS respectively to experiment the feasibility of anomaly-based approaches for IoMT security. They showed how analyzing device data packets and network traffic using machine learning algorithms like fuzzy classifiers and decision trees can accurately identify abnormal behaviors indicative of attacks. This aligns with the study's goal of using machine learning to predict cyber threats patterns on the network. However, [48] emphasize the importance of selecting suitable machine learning algorithms and IoMT-specific datasets for training IDS models. Their use of the realistic WUSTL-EHMS-2020 dataset highlights the need for comprehensive data that includes both network features and device/patient information, which significantly improves detection performance by integrating multiple data dimensions.

2.5 Chosen Machine Learning Models

SVM and GBM machine learning models were chosen for threats prediction in this study. The choice of SVM and GBM models is motivated by their proven effectiveness in high-dimensional spaces and their ability to model complex, nonlinear relationships that are characteristic of cyber-physical attack vectors on medical devices. SVM predicts network threats by classifying network traffic patterns as either normal or malicious based on the optimal hyperplane that separates these classes in the feature space [46]. GBM predicts network threats by sequentially building models that correct the errors of previous models, thereby identifying complex patterns and interactions in network traffic indicative of malicious activity [49].

3. RESEARCH METHODOLOGY

In this section, the dataset features are discussed which includes biometric features, network traffic features and label features. Also discussed in this section are the step-by-step methods implemented for predicting potential cyber threats using SVM and GBM models which includes data collection, data preprocessing, feature engineering, model selection, training, and evaluation.

3.1 Dataset

This study utilizes the WUSTL-EHMS-2020 dataset, rich in quantitative data such as network traffic features, biometric data, and attack labels. This numerical data facilitates objective measurement, statistical analysis, and empirical validation of hypotheses, which are the key features of quantitative research [49], [50]. Also, the quantitative approach aligns with the study's objective of utilizing predictive analytics for potential security breaches [50]. The dataset used for this study is the Washington University in St. Louis EHMS 2020 referred to as the WUSTL-EHMS-2020 dataset [48], [51]. This dataset was selected for this study because it was already pre-collected, organized and was suitable for the study's objective to utilize machine learning to predict potential security breaches in pacemaker

devices by analyzing cyber trends and patterns in network [52]. Also, the dataset provides detailed information, including network traffic features and patients' biometric data and attack labels.

3.1.1. Dataset Description

The dataset comprises 16,318 records. Each record is a unique instance representing a combination of network and biometric data points, which are labeled under 'Normal' operations or 'Attack' scenarios. The features of the dataset are described below.

Biometric Data Features: (Temp), measures the body temperature of the patient. Oxygen Saturation (SpO₂), measures percentage of hemoglobin binding sites in the bloodstream occupied by oxygen. (Pulse_Rate), measures the number of heart beats per minute. Systolic Blood Pressure (SYS), measures the maximum arterial pressure during contraction of the left ventricle of the heart. Diastolic Blood Pressure (DIA), measures the minimum arterial pressure during relaxation and dilatation of the ventricles of the heart when they fill with blood. (Heart_Rate), measures the frequency of heartbeats. Respiration Rate (Resp_Rate), measures the rate at which breathing occurs. ST Segment (ST), part of the heart's electrical activity recorded during a cardiac cycle.

Network Traffic Features: Dir, indicating direction of the traffic flow. SrcAddr, source IP address from which the packet originated. DstAddr, destination IP address to which the packet is being sent. Sport, Source port number, indicating the port from which the packet was sent. Dport, destination port number, indicating the port to which the packet is being sent. SrcBytes, number of bytes sent from the source to the destination. DstBytes, number of bytes sent from the destination to the source. SrcLoad (Source Load) and DstLoad (Destination Load), indicate the load on source and destination, useful for detecting overloads or unusual activity. SIntPkt, inter-packet arrival time for packets sent from the source. SIntPkt (Source Inter-packet Time) and DIntPkt (Destination Inter-packet Time), time between packets, which can help identify timing-based anomalies. SrcJitter (Source Jitter) and DstJitter (Destination Jitter), variation in packet arrival times, useful for identifying irregularities in traffic flow. Loss, number of packets lost during the transmission. pLoss, percentage of packets lost during the transmission. Rate, data transfer rate. SrcLoad, load on the source in terms of the amount of data being sent. DstLoad, load on the destination in terms of the amount of data being received. Flgs, flags set in the packet, which are used to control or identify certain conditions or features of the packet. SrcMac: MAC (Media Access Control) address of the source device.

Label Feature

Out of the 16,318 records, 14,272 are categorized as 'Normal' indicated by label '0', signifying typical, safe operations. While 2,046 records, indicated by label '1' are marked under various 'Attack' categories, indicating Spoofing attack or Data Alteration.

3.2 Ethical Considerations

The WUSTL-EHMS-2020 dataset is publicly accessible via the Washington University in St. Louis portal [51]. The provision of this dataset is governed by the Creative Commons Attribution 4.0 License, as outlined on their official licensing page [53]. The data was explicitly consented for use as stated by [48], ensuring compliance with the stipulated usage terms and ethical guidelines.

3.3 Methodology

This section discusses the step-by-step method for predicting potential cyber threats using SVM and GBM models to analyze cyber trends and patterns on the pacemaker device network. These steps include data collection, implementation setup, Importing libraries, data preprocessing, model training and evaluation.

3.3.1 Data Collection

The WUSTL-EHMS-2020 dataset that was used for the machine learning prediction was obtained from the Washington University in St. Louis portal [51]. This WUSTL-EHMS-2020 dataset was generated by [48], using a real-time EHMS testbed that collects both network traffic features and patients' biometric data. The dataset consists

of network features, biometric data of patients and labels for attack types, data alteration and spoofing as can be seen in Figure 3.

3.3.2 Implementation Setup Environment

The machine learning implementation was performed using HP EliteBook 840 G5 laptop running Microsoft Windows 10 Enterprise operating system on an x64-based PC architecture. The Jupyter Notebook 6.5.4 Integrated Development Environment (IDE) accessed through the Anaconda Navigator Graphical User Interface (GUI) [54], was used to implement the Support Vector Machine (SVM) and Gradient Boosting Machine (GBM) machine learning algorithms to predict cyber threats on the pacemaker device network. This IDE facilitated effective training, evaluation, and visualization of the machine learning models. The python programming language was used, and its libraries include pandas, scikit-learn, numpy, seaborn, and matplotlib.

3.3.1 Data Preprocessing

The data preprocessing stage involves cleaning the dataset by identifying and correcting inaccurate entries from the dataset, to enhance the machine learning model's performance [55]. The data preprocessing steps include the following:

- i. Handling missing values of the dataset by replacing missing values in numerical columns with the median and converting categorical columns into binary format [55].
- ii. Performing 5-fold cross-validation was used to validate the models' performances by testing models' accuracy on the training and testing subsets of the data [48].

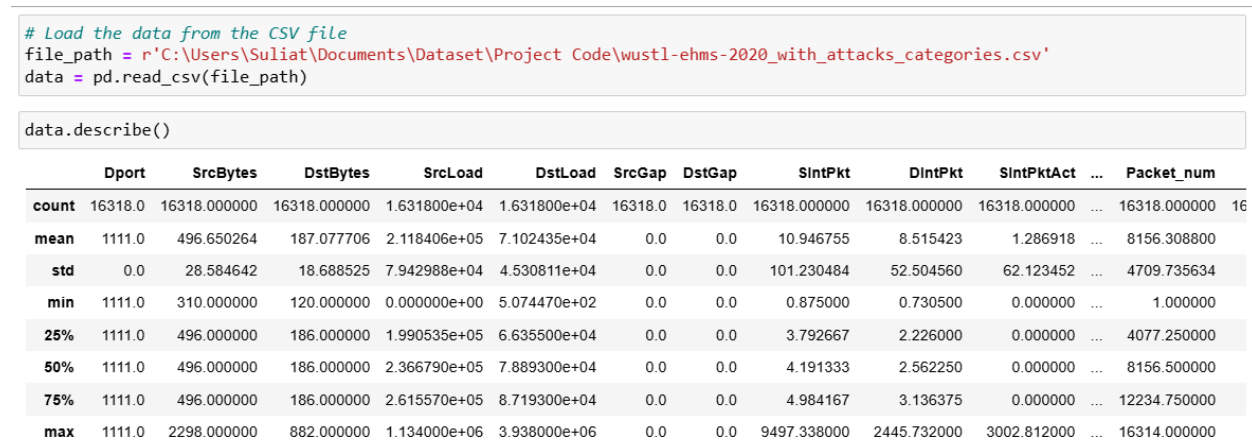


Figure 3. The Wustl-ehms-2020_with_attacks_categories Dataset

3.4 Feature Engineering

Feature engineering involves selecting necessary features from the dataset and normalizing the selected features for quick processing and improved training performance [43]. Feature engineering improves models' performance by transforming raw data into a format that is better suited for analysis. The next few sections explain the processes of feature engineering.

3.4.1 Feature Selection

The feature selection involves selecting relevant dataset features and transforming the features to improve models' performance [55]. This include encoding categorical variables like 'Flgs' and 'SrcMac' into numerical format, using one-hot encoder.

3.4.2 Data Normalization

Data normalization modifies the range of numerical features of the dataset like 'SrcLoad' and 'DstLoad', to a common scale, usually between zero and one [57].

3.4.3 Data Splitting

Data splitting involves dividing the dataset into two training set and testing set to improve models' performance [48]. The dataset was divided into the ratio of 80% and 20%, where 80% is for training and 20% for testing [58]. This 80% - 20% data splitting approach mitigates overfitting, and evaluates how well the model performs on new, unseen data[58].

3.4.4 Model Selection

The SVM and GBM models were selected because they suit the problem being addressed. SVM is suitable in handling high-dimensional data with numerous features and indicators effectively [59], like the Wustl-ehms-2020 dataset. SVM can also perform non-linear classification and maximizes margins between classes, thereby enhancing its generalization capability [59]. GBM is effective for predicting cybersecurity threats due to its ability to process and integrate heterogeneous data types found in network datasets [60] like the Wustl-ehms-2020 dataset. Also, GBMs improve predictive accuracy by sequentially constructing decision trees where each of these trees aims to address the errors made by the prior one [60].

3.5 Model Training

Training the SVM and GBM models entails a series of systematic steps to enable the algorithms effectively learn from the data and make accurate predictions. Training of these machine learning models provides real-time monitoring capabilities, enabling quick detection of anomalies that may signal potential cyber-attacks, and response to these attacks [15]. In SVM model training the first step involves choosing the suitable kernel type that best suits the dataset, and then configuring the SVM model by creating hyperplane to effectively classify the data points [46]. The GBM approach differs from others in that it trains a series of decision trees [61]. Each tree is specifically designed to address the errors made by the prior one.

3.6 Model Evaluation

The performance of the trained models was evaluated using the testing dataset. The evaluation results of SVM and GBM show how well these models perform on unseen data. TP (True Positives)- number of instances correctly classified as positive. TN (True Negatives)- number of instances correctly classified as negative. FP (False Positives)- number of instances incorrectly classified as positive. FN (False Negatives)- number of instances incorrectly classified as negative.

Accuracy: Calculates the proportion of total correct predictions against all predictions made [62], [44] (see Equation (1)).

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision: Calculates the accuracy of the models' positive [62], [44]. Precision is false positives is high, precision is particularly critical (see Equation (2)).

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

Recall: Evaluates relevant instances identified by the models (true positive rate) [62], [44] (see Equation (3)).

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

F1-Score: Combines precision & recall, and calculates their harmonic mean [62], [44]. It is especially useful when dealing with imbalanced datasets (see Equation (4)).

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{4}$$

Confusion Matrix: The confusion matrix as illustrated in Figure 4. describes the model's performance by comparing its actual and predicted classes [46].

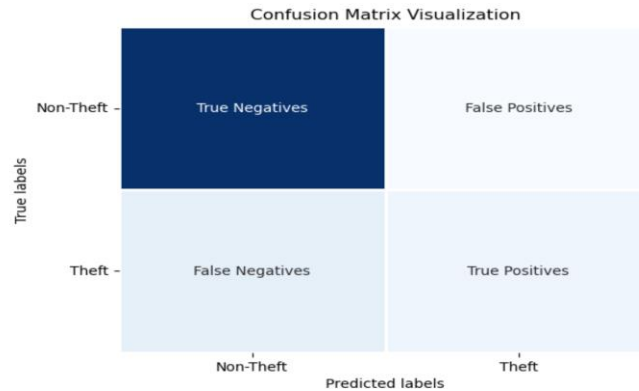


Figure 4. Confusion Matrix Visualization

4 IMPLEMENTATION RESULTS

This section demonstrates the implementation results, including the trend results in biometric data, simulation results of predictive model, and results of the SVM & GBM confusion matrices. The "Wustl-ehms_2020_with_attacks_categories" dataset was used to train SVM & GBM models to recognize patterns associated with various attack vectors and normal operation. The 'Label' column in the dataset has two categories, represented by the integers 0 and 1. Below is the distribution of these categories as shown in Figure 5: Label 0: There are 14,272 instances categorized as '0', which typically represents normal, non-attack scenarios. Label 1: There are 2,046 instances categorized as '1', which represents some form of attack or anomaly.

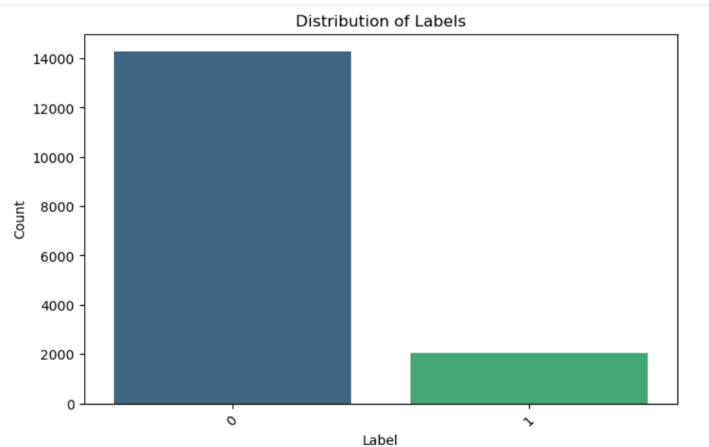


Figure 5. Distribution of Labels

4.1 Result of the Predictive Models

The Jupyter notebook IDE was used to perform data handling and visualization of the simulation results, using python libraries such as scikit-learn, pandas, numpy, Seaborn and Matplotlib. These were used for plotting accuracy, precision, and recall curves, thereby providing a comprehensive view of the models' performance. The bar chart in Figure 6 Model Performance Comparison illustrates the comparison of the SVM and GBM models' performance against the combined network and biometric data. The performance metrics as shown are accuracy, precision, recall, and F1_score represented by blue, orange, green, and red bars, respectively.

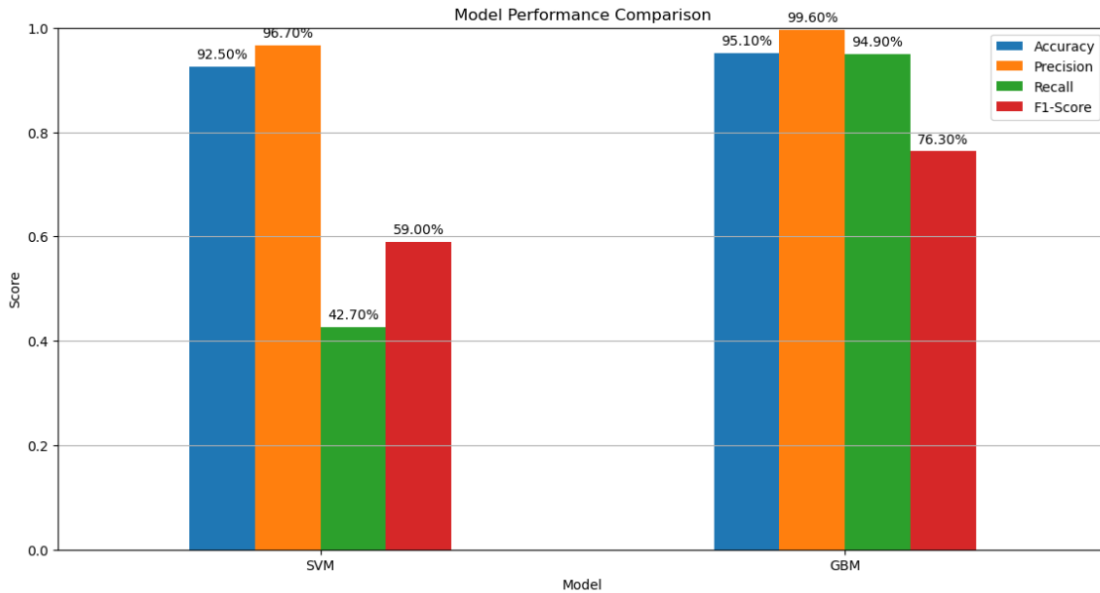


Figure 6. Model Performance Comparison

Figure 7 shows the results of Confusion Matrix visualization results based on the performance of a SVM classifier. It shows the actual versus predicted classifications for two classes: Normal and Attack. The matrix reveals that the classifier correctly predicted 2,842 instances as Normal and 178 instances as Attack. However, it misclassified 6 instances of Normal as Attack and 238 instances of Attack as Normal.

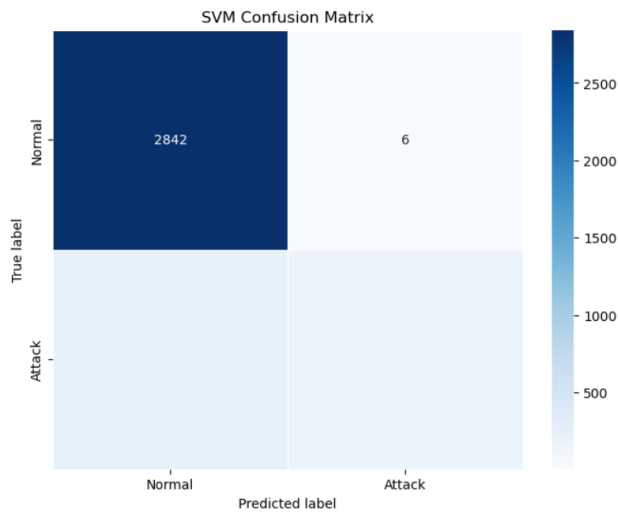


Figure 7. SVM Model Confusion Matrix

Figure 8 shows performance evaluation of a GBM classifier. It shows the actual versus predicted classifications for two classes: Normal and Attack. The matrix indicates that the classifier perfectly predicted all instances, with 2,854 instances correctly classified as Normal and 253 instances correctly classified as Attack. It misclassified 1 instance of Normal as Attack and 156 instances of Attack as Normal. Figure 9 shows the pie chart illustration of the confusion matrices for GBM and SVM classifiers.

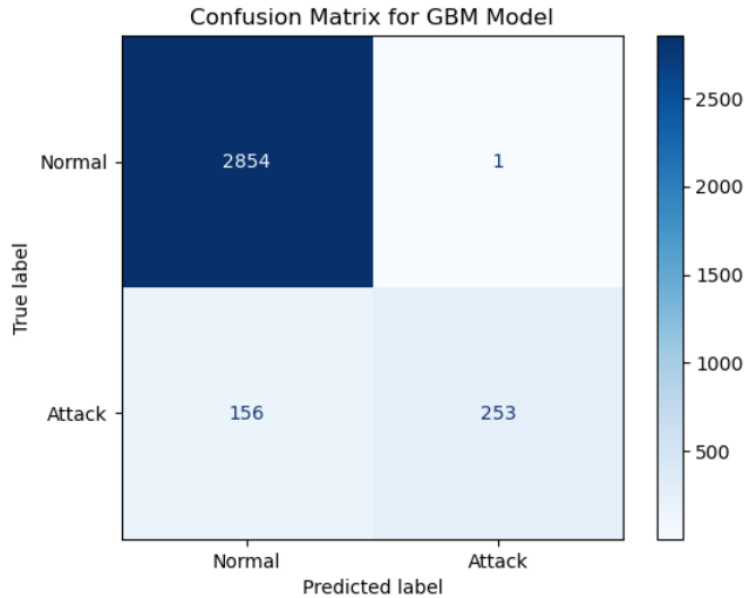


Figure 8. GBM Model Confusion Matrix

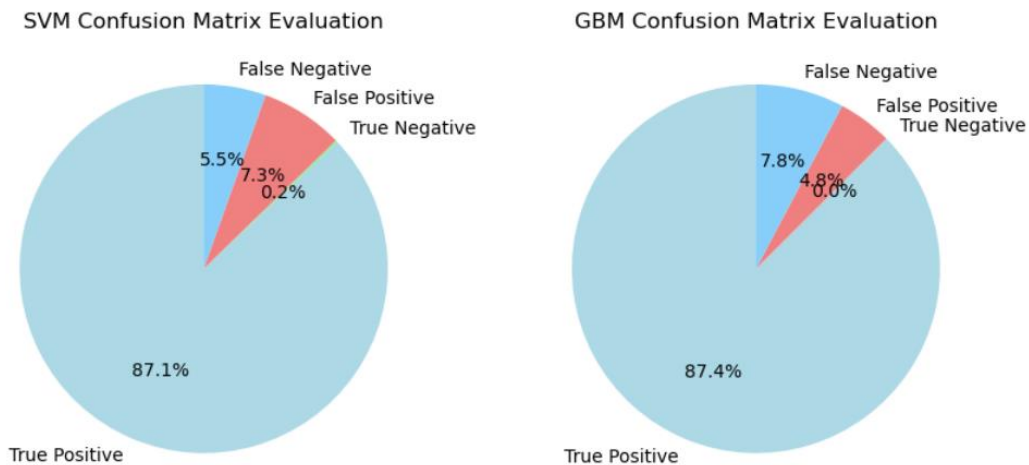


Figure 9. Pie-chart Illustration Of SVM And GBM Confusion Matrices

5 DISCUSSIONS

This section provides analysis of the dataset and biometric trends, compares model performances, discusses the implications of the results, evaluates the effectiveness of the SVM and GBM models, and aligns the models' implementation results with research questions. The dataset includes network traffic features, biometric data, and

attack categories. The objective is to identify trends in the biometric data and analyze the distribution and impact of different attack categories.

5.1 Comparative Analysis of Models Performance Using Evaluation Results

- **Accuracy:** The GBM model outperformed the SVM model in terms of accuracy. While the SVM model has an accuracy of 92.50%, the GBM model achieved a higher score of 95.1%.
- **Precision:** Similarly, the GBM model has a higher precision score of 99.6%, outperforming the SVM model which has a precision of 96.70%. This shows that GBM is better at making accurate positive predictions.
- **Recall:** The recall for the GBM model is significantly higher at 94.90%, compared to the SVM model's recall of 42.70%. This shows that GBM is much better at identifying all actual positive cases, whereas the SVM model misses a substantial number of positive cases.
- **F1 Score:** The GBM model has an F1 score of 76.30%, while SVM model has a lower F1 score of approximately 59.00%, indicating a trade-off between precision and recall, with recall being notably lower.

Based on the experimental results, the analysis shows that GBM model demonstrates superior performance across all the evaluated metrics (accuracy, precision, recall and F1 score) compared to the SVM model. GBM's superiority in accuracy and recall can be attributed to its iterative correction of errors from previous trees, which makes it highly effective for complex datasets where patterns and anomalies are not immediately apparent. This adaptability is crucial in medical device security, where new types of attacks may emerge that are not explicitly covered in the training data. The ability of GBM to handle heterogeneous data and its robustness against overfitting also contribute to its higher performance metrics [59]. While SVM showed a high precision, its lower recall rate suggests that it is less effective at identifying all actual positives, which in this context means detecting all real threats. This is partly because SVMs are sensitive to the choice of kernel and the regularization parameter. In an imbalanced dataset like the one employed in this study, where 'Normal' instances far outnumber 'Attack' instances, SVM struggles to identify the less frequent positive class. Therefore, the GBM model is the better-performing model in this comparison.

5.2 Comparative Analysis of Models Performance

This section compares the analysis of the confusion matrices in figures 7 & 8 for the SVM and GBM models' classifiers to evaluate their performance in predicting cyber-attacks. GBM Confusion Matrix: Figure 7. shows that the GBM classifier achieved classification with 253 True Positives (TP), 1 False Positives (FP), 2,854 True Negatives (TN), and 156 False Negatives (FN). SVM Confusion Matrix: In Figure 7, the SVM classifier shows 178 True Positives (TP), 6 False Positives (FP), 2,842 True Negatives (TN), and 238 False Negatives (FN). This shows that while the SVM model has high accuracy, it has a substantial number of false negatives, thereby reducing its recall performance compared to the GBM model. Based on Figure 9, the analysis of the confusion matrix distributions for the SVM and GBM models in detecting cyber threats shows significant differences in their performance. Both models show a high proportion of true positives, with GBM slightly higher at 87.4% compared to SVM at 87.1%. This demonstrates that both models are effective in correctly detecting genuine threats. However, GBM outperformed SVM in minimizing false positives, with rates of 4.8% and 7.3%, respectively. Lower false positives mean fewer unnecessary alerts and interventions, which is essential in a medical context to avoid causing undue stress to patients and reducing the workload on healthcare providers. SVM has more value in terms of false negatives, with a lower rate of 5.5% compared to GBM's 7.8%. For pacemaker devices, false negatives are essential as they represent missed threats that could lead to device malfunctions and threat patients' lives.

5.3 Comparison of Experimental Results with Related Work that Utilized Same Dataset

GBM model in this study has demonstrated high performance across all evaluation metrics, which are essential for minimizing false positives and false negatives in a healthcare context. [48], utilized the WUSTL-EHMS-2020 dataset. While GBM is not evaluated in their study, the best performing model, Artificial Neural Network (ANN) shows a high AUC- 92.98%, thereby illustrating the importance of using combined features (network and biometric data) for improving detection capabilities. This use of combined features aligns with the superior results obtained with GBM model in this study. In conclusion, GBM shows better overall performance compared to SVM and potentially other models like RF and KNN when considering precision and recall, critical factors for healthcare systems. ANN presents

strong AUC results, GBM's high precision and recall make it a particularly effective choice for scenarios where accurate detection of anomalies is most important.

5.4 Comparative Analysis of SVM Performance with Other Study

This study demonstrates SVM performance with an accuracy of 92.50%, a precision of 96.70%, but a lower recall of 42.70% and an F1-score of 59.00%. This indicates that while the SVM model is highly precise in predicting non-attack scenarios accurately, it struggles with detecting all positive attack cases, as indicated by the low recall. Authors in [63], reports an overall accuracy of 77.5%, sensitivity (recall) of 0.62, and specificity of 0.86. These metrics indicate a more balanced performance between identifying positive cases and avoiding false positives. The lower accuracy compared to the first study might reflect the complexity and variability inherent in predicting medical conditions, where factors influencing cardiovascular diseases can be diverse and multifactorial. The higher specificity compared to sensitivity shows that SVM model was better at correctly identifying false negatives. While both studies showcase effective uses of SVM in their respective fields, the choice of SVM configuration and the resulting trade-offs in performance metrics should be carefully considered based on the specific requirements of the application environment. The GBM model was utilized as an additional machine learning technique. This is justified by the model's ability to handle heterogeneous data types effectively and its sequential learning approach, which corrects errors made by previous trees, enhancing overall predictive accuracy. The comparative analysis of the SVM and GBM models demonstrated that GBM significantly outperformed SVM in terms of the key performance metrics, including accuracy, precision, recall, and F1 score. Specifically, GBM achieved an accuracy of 95.1% compared to SVM's 92.5%.

6 CONCLUSION

This study has demonstrated the necessity for improved pacemakers' cybersecurity, with increasing vulnerability to cyber threats due to their advanced wireless capabilities. The study has provided a comprehensive overview of cybersecurity vulnerabilities associated with pacemaker devices and recommended mitigation strategies for these vulnerabilities. One of the key mitigation strategies identified is the use of Machine Learning to analyze and predict cyber threats, thereby aligning with its stated objectives.

The research methodology employed a quantitative research approach using the WUSTL-EHMS-2020 dataset, comprising of network traffic features and patients' biometric data and attack label, to train machine learning models for predicting cyber threats. The step-by-step methods of machine learning prediction includes data collection, data preprocessing, feature engineering, and model training using SVM and GBM models. The evaluation results showed that the GBM model significantly outperformed the SVM across all evaluation metrics - accuracy (95.1% vs 92.5%), precision (99.60% vs 96.7%), recall (94.90% vs 42.7%), and F1 score (76.30% vs 59.00%). The confusion matrices visually indicate that the GBM model outperformed the SVM model in correctly classifying both positive and negative cases, with fewer misclassifications and higher overall accuracy.

6.1 Limitations

This study presents a comprehensive method to strengthen pacemaker cybersecurity through machine learning-based intrusion detection. While the WUSTL-EHMS-2020 dataset is comprehensive, it may not fully represent the entire spectrum of real-world scenarios and attack vectors. This study focused on SVM and GBM models. While these models demonstrated promising results, other algorithms or ensemble techniques may offer different trade-offs or performance characteristics that were not explored. This study did not fully assess the performance implications or needs for computational resources while implementing machine learning prediction in a real-world setting. While this study provided valuable insights through simulations and evaluations, the proposed countermeasures have not undergone extensive real-world testing or validation in healthcare facilities or with actual pacemaker devices. Factors such as environmental conditions, user interactions, and unforeseen edge cases may influence the performance and effectiveness of the proposed solutions in practical deployments. Also, this study did not attempt to handle imbalanced classes of the dataset using oversampling/undersampling methods that might improve the models' performances.

6.2 Future Recommendations

Integrating GBM model into pacemaker security framework can enable real-time monitoring and early detection of potential cyber-attacks or anomalies [49] [64]. As new cyber threats emerge, it is crucial to update the GBM model with the latest attack patterns and biometric data trends [41]. Machine learning techniques should be integrated with existing pacemaker devices security measures, like encryption, access control mechanisms, authentication protocols, and blockchain technology [41]. Compliance with regulations such as the HIPAA in the U.S. and the GDPR in Europe is necessary for ensuring data privacy in medical devices [64] [32]. Both regulations set forth standards and requirements that help protect sensitive health information, which is relevant for connected medical devices like pacemakers. The healthcare professionals, patients, and other stakeholders should be educated about the importance of cybersecurity in medical devices [65]. Providing training on best practices for secure handling, monitoring, and reporting of potential cyber threats or detected anomalies, can promote a culture of cyber vigilance and collaboration in protecting pacemaker devices. Implementing routine cybersecurity risk assessment process to identify potential vulnerabilities in the pacemaker ecosystem, including the pacemaker device, communication network, and supporting infrastructure, can help ensure compliance with established security protocols and identify areas for improvement [13]. Auditing key cybersecurity controls in pacemakers like configuration management, vulnerability management, patch management, access controls, and incident response plans is essential to evaluate their effectiveness and ensure compliance. There should be a detailed plan ready to address potential cybersecurity breaches or attacks targeting pacemakers [15]. Given the critical life-sustaining function of these devices, a comprehensive incident response strategy is essential to mitigate risks and protect patient safety.

ACKNOWLEDGEMENT

The authors received no funding from any party for the research and publication of this article. Implementation codes are available at: <https://github.com/Suliat247/Predicting-Cyber-Threats-in-Pacemaker-Devices-Using-Machine-Learning>

AUTHOR CONTRIBUTIONS

Suliat Toyosi Jimoh: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation.

Shaymaa Al-Juboori: Project Supervision, Writing – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests was disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. <https://publicationethics.org/>

REFERENCES

- [1] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare," *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 18, no. 14, p. 155079, 2018, doi: 10.4108/eai.13-7-2018.155079.
- [2] D. Lee and S. N. Yoon, "Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenges," *International Journal of Environmental Research and Public Health*, vol. 18, no. 1, p. 271, 2021, doi: 10.3390/ijerph18010271.
- [3] P. Li, G.-H. Lee, S. Y. Kim, S. Y. Kwon, H.-R. Kim, and S. Park, "From Diagnosis to Treatment: Recent Advances in Patient-Friendly Biosensors and Implantable Devices," *ACS Nano*, vol. 15, no. 2, pp. 1960–2004, 2021, doi: 10.1021/acsnano.0c06688.


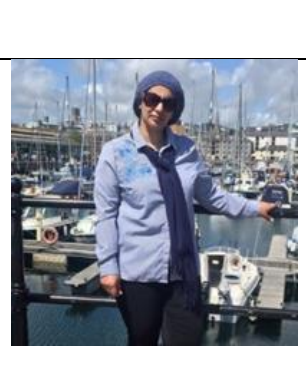
- [4] X. Chen *et al.*, “Stretchable Supercapacitors as Emergent Energy Storage Units for Health Monitoring Bioelectronics,” *Advanced Energy Materials*, vol. 10, no. 4, 2019, doi: 10.1002/aenm.201902769.
- [5] M. Kintzlinger *et al.*, “CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices,” *IEEE Access*, vol. 8, pp. 48123–48140, 2020, doi: 10.1109/access.2020.2978631.
- [6] J.-P. O. Li *et al.*, “Digital technology, tele-medicine and artificial intelligence in ophthalmology: A global perspective,” *Progress in Retinal and Eye Research*, vol. 82, p. 100900, 2020, doi: 10.1016/j.preteyeres.2020.100900.
- [7] M. Kintzlinger *et al.*, “CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices,” *IEEE Access*, vol. 8, pp. 48123–48140, 2020, doi: 10.1109/access.2020.2978631.
- [8] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, “An investigation and comparison of machine learning approaches for intrusion detection in IoMT network,” *Journal of Supercomputing*, vol. 78, pp. 17403–17422, 2022, doi: [10.1007/s11227-022-04568-3](https://doi.org/10.1007/s11227-022-04568-3).
- [9] M. Ibrahim, A. Alsheikh, and A. Matar, “Attack Graph Modeling for Implantable Pacemaker,” *Biosensors*, vol. 10, no. 2, p. 14, 2020, doi: 10.3390/bios10020014.
- [10] A. Panda, S. Pinisetty, and P. Roop, “Securing Pacemakers using Runtime Monitors over Physiological Signals,” *ACM Transactions on Embedded Computing Systems*, 2024, doi: 10.1145/3638286.
- [11] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459-182476, 2019, doi: 10.1109/ACCESS.2019.2960412.
- [12] A. Kapoor, A. Vora, and R. Yadav, “Cardiac devices and cyber attacks: How far are they real? How to overcome?,” *Indian Heart Journal*, vol. 71, no. 6, pp. 427–430, Nov. 2019, doi: 10.1016/j.ihj.2020.02.001.
- [13] M. Ngamboé, P. Berthier, N. Ammari, K. Dyrda, and J. M. Fernandez, “Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED),” *International Journal of Information Security*, vol. 20, no. 4, pp. 621–645, 2020, doi: 10.1007/s10207-020-00522-7.
- [14] N. M. Thomasian and E. Y. Adashi, “Cybersecurity in the Internet of Medical Things,” *Health Policy and Technology*, vol. 10, no. 3, p. 100549, Jul. 2021, doi: 10.1016/j.hlpt.2021.100549.
- [15] T. C., V. Bhanu S., and S. S., “Ensuring Communication Network Security for Medical Implantable Devices to Enhance Cyber Security,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 2, pp. 486–494, 2023. [Online]. Available: <https://www.ijisae.org/index.php/IJISAE/article/view/4293>.
- [16] L. Pycroft and T. Z. Aziz, “Security of implantable medical devices with wireless connections: The dangers of cyber-attacks,” *Expert Review of Medical Devices*, vol. 15, no. 6, pp. 403–406, 2018, doi: 10.1080/17434440.2018.1483235.
- [17] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, “Survey of Machine Learning based intrusion detection methods for Internet of Medical Things,” *Applied Soft Computing*, vol. 140, p. 110227, 2023, doi: 10.1016/j.asoc.2023.110227.
- [18] Y. He, A. Aliyu, M. Evans, and C. Luo, “Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review,” *Journal of Medical Internet Research*, vol. 23, no. 4, p. e21747, 2021, doi: 10.2196/21747.
- [19] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, “Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML,” *Journal of Network and Computer Applications*, vol. 201, p. 103332, 2022, doi: 10.1016/j.jnca.2022.103332.
- [20] I. Ahmed, H. Karvonen, T. Kumponiemi, and M. Katz, “Wireless Communications for the Hospital of the Future: Requirements, Challenges and Solutions,” *International Journal of Wireless Information Networks*, vol. 27, no. 1, pp. 4–17, Oct. 2019, doi: 10.1007/s10776-019-00468-1.
- [21] R. Hireche, H. Mansouri, and A.-S. K. Pathan, “Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis,” *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 640–661, 2022, doi: 10.3390/jcp2030033.
- [22] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, “Identifying the attack surface for IoT network,” *Internet of Things*, vol. 9, p. 100162, 2020, doi: 10.1016/j.iot.2020.100162.

- [23] G. Zheng *et al.*, "Finger-to-Heart (F2H): Authentication for Wireless Implantable Medical Devices," in *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 4, pp. 1546-1557, 2019, doi: 10.1109/JBHI.2018.2864796.
- [24] Woodholme Cardiovascular Associates, "Pacemaker," 2024. [Online]. Available: <https://woodholmecardio.com/services/pacemaker/>.
- [25] M. Kintzlinger and N. Nissim, "Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems," *Journal of Biomedical Informatics*, vol. 95, p. 103233, 2019, doi: 10.1016/j.jbi.2019.103233.
- [26] B. Vandenberk and S. R. Raj, "Remote Patient Monitoring: What Have We Learned and Where Are We Going?," *Current Cardiovascular Risk Reports*, vol. 17, no. 6, pp. 103–115, 2023, doi: 10.1007/s12170-023-00720-7.
- [27] P. Pritika, B. Shanmugam, and S. Azam, "Risk Assessment of Heterogeneous IoMT Devices: A Review," *Technologies*, vol. 11, no. 1, p. 31, 2023, doi: 10.3390/technologies11010031.
- [28] M. Elhoseny *et al.*, "Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions," *Sustainability*, vol. 13, no. 21, p. 11645, 2021, doi: 10.3390/su132111645.
- [29] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1–44, 2021, doi: 10.1145/3453176.
- [30] Y. Yamout, T. S. Yeasar, S. Iqbal, and M. Zulkernine, "Beyond Smart Homes: An In-Depth Analysis of Smart Aging Care System Security," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–35, 2023, doi: 10.1145/3610225.
- [31] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (IoT) network at device-level," *Internet of Things*, vol. 11, p. 100240, 2020, doi: 10.1016/j.iot.2020.100240.
- [32] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)," *Applied Sciences*, vol. 12, no. 4, p. 1927, 2022, doi: 10.3390/app12041927.
- [33] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," in *IEEE Access*, vol. 4, pp. 959-979, 2016, doi: 10.1109/ACCESS.2016.2521727.
- [34] I. Stine, M. Rice, S. Dunlap, and J. Pecarina, "A cyber risk scoring system for medical devices," *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 32–46, 2017, doi: 10.1016/j.ijcip.2017.04.001.
- [35] L. Wu, X. Du, M. Guizani and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272-1283, 2017, doi: 10.1109/JIOT.2017.2708042.
- [36] J. Fiaidhi and S. Mohammed, "Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies," in *IT Professional*, vol. 21, no. 4, pp. 48-55, 2019, doi: 10.1109/MITP.2019.2906442.
- [37] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723-3768, 2019, doi: 10.1109/COMST.2019.2914094.
- [38] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao and K. Saleem, "Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review," in *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562-576, 2017, doi: 10.1109/JSEN.2016.2633973.
- [39] E. Kwarteng and M. Cebe, "A survey on security issues in modern Implantable Devices: Solutions and future issues," *Smart Health*, vol. 25, p. 100295, 2022, doi: 10.1016/j.smhl.2022.100295.
- [40] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," *Frontiers in Digital Health*, vol. 4, 2022, doi: 10.3389/fgdth.2022.862221.
- [41] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

- [42] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, 2022, doi: 10.3390/jcp2030027.
- [43] M. Zubair *et al.*, "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System," *Sensors*, vol. 22, no. 21, p. 8280, 2022, doi: 10.3390/s22218280.
- [44] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, and B. Bhushan, "A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022, doi: 10.3390/su141912828.
- [45] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li and Z. J. Cao, "A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4260-4269, 2021, doi: 10.1109/TII.2020.3011444.
- [46] G. Zachos, I. Essop, G. Mantas, K. Porfyraakis, J. C. Ribeiro, and J. Rodriguez, "An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks," *Electronics*, vol. 10, no. 21, p. 2562, 2021, doi: 10.3390/electronics10212562.
- [47] G. Thamilarasu, A. Odesile and A. Hoang, "An Intrusion Detection System for Internet of Medical Things," in *IEEE Access*, vol. 8, pp. 181560-181576, 2020, doi: 10.1109/ACCESS.2020.3026260.
- [48] 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," in *IEEE Access*, vol. 8, pp. 106576-106584, 2020, doi: 10.1109/ACCESS.2020.3000421.
- [49] H. Taherdoost, "What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations," *Journal of Management Science & Engineering Research*, vol. 5, no. 1, pp. 53–63, 2022, doi: 10.30564/jmsr.v5i1.4538.
- [50] M. Hassan, "Quantitative Research – Methods, Types and Analysis," 2024. [Online]. Available: <https://researchmethod.net/quantitative-research/>.
- [51] WUSTL, "Washinton University in St. Louis," 2020. [Online]. Available: <https://www.cse.wustl.edu/~jain/ehms/index.html>. [Accessed 2024].
- [52] V. Ravi, T. D. Pham, and M. Alazab, "Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 50–54, Jun. 2023, doi: 10.1109/iotm.001.2300021.
- [53] Creative Commons, "CC BY 4.0 DEED - Attribution 4.0 International," 2020. [Online]. Available: <https://creativecommons.org/licenses/by/4.0/deed.en>.
- [54] Anaconda, "The Operating System for AI," 2024. [Online]. Available: <https://www.anaconda.com/>.
- [55] M. Alalhareth and S.-C. Hong, "An Improved Mutual Information Feature Selection Technique for Intrusion Detection Systems in the Internet of Medical Things," *Sensors*, vol. 23, no. 10, p. 4971, 2023, doi: 10.3390/s23104971.
- [56] Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 161546-161554, 2021, doi: 10.1109/ACCESS.2021.3128837.
- [57] A. Abdo, R. Mostafa, and L. Abdel-Hamid, "An Optimized Hybrid Approach for Feature Selection Based on Chi-Square and Particle Swarm Optimization Algorithms," *Data*, vol. 9, no. 2, p. 20, 2024, doi: 10.3390/data9020020.
- [58] F. Khan, X. Yu, Z. Yuan, and A. U. Rehman, "ECG classification using 1-D convolutional deep residual neural network," *PLoS ONE*, vol. 18, no. 4, p. e0284791, 2023, doi: 10.1371/journal.pone.0284791.
- [59] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

- [60] P. Verma *et al.*, “A Novel Intrusion Detection Approach Using Machine Learning Ensemble for IoT Environments,” *Applied Sciences*, vol. 11, no. 21, p. 10268, 2021, doi: 10.3390/app112110268.
- [61] A. Rehman, T. Alam, M. Mujahid, F. S. Alamri, B. A. Ghofaily, and T. Saba, “RDET stacking classifier: a novel machine learning based approach for stroke prediction using imbalance data,” *PeerJ Computer Science*, vol. 9, p. e1684, 2023, doi: 10.7717/peerj-cs.1684.
- [62] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, “Security of Things Intrusion Detection System for Smart Healthcare,” *Electronics*, vol. 10, no. 12, p. 1375, 2021, doi: 10.3390/electronics10121375.
- [63] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, “An accurate and dynamic predictive model for a smart M-Health system using machine learning,” *Information Sciences*, vol. 538, pp. 486–502, 2020, doi: 10.1016/j.ins.2020.06.025.
- [64] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, “A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches,” *PeerJ Computer Science*, vol. 7, p. e414, 2021, doi: 10.7717/peerj-cs.414.
- [65] S. T. Argaw *et al.*, “Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks,” *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, 2020, doi: 10.1186/s12911-020-01161-7.

BIOGRAPHIES OF AUTHORS

	<p>Suliat Toyosi Jimoh holds an MSc in Cyber Security from the University of Plymouth and a BSc in Information Technology from Kebbi State University of Science & Technology, Aliero. Her work focuses on using Machine Learning to improve cybersecurity. Suliat has experience in network security and IT solutions, and she conducts training sessions on cybersecurity awareness. She is a member of the Chartered Institute of Information Security (CIISec). You can reach Suliat at toyosi.suliat@gmail.com or connect with her on LinkedIn.</p>
	<p>Dr. Shaymaa Al-Juboori is a lecturer in the Computer Science department at the University of Plymouth, she holds a Ph.D. in EEG healthcare applications from the University of Plymouth, Plymouth, U.K., the M.Sc. degree in digital signal processing from the University of Technology, Baghdad, Iraq, and the B.Sc. degree in Electrical Engineering. She has published premium research papers in the area of healthcare applications using machine learning, including book chapters and presented at international conferences.</p>