sustainability

MDPI

Article

A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things

Rajasekhar Chaganti [1,*], Azrour Mourade [2], Vinayakumar Ravi [3], Naga Vemprala [4], Amit Dua [5] and Bharat Bhushan [6]

[1] Toyota Research Institute, Los Altos, CA 94022, USA
[2] Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismail University, Meknes 50050, Morocco
[3] Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Al-Khober 34754, Saudi Arabia
[4] Pamplin School of Business, University of Portland, Portland, OR 97203, USA
[5] Department of Algorithmics and Software, Silesian University of Technology, 44-100 Gliwice, Poland
[6] Department of Computer Science and Engineering, School of Engineering and Technology (SET), Sharda University, Greater Noida, Uttar Pradesh 201310, India
* Correspondence: raj.chaganti2@gmail.com

Abstract: Integrating the internet of things (IoT) in medical applications has significantly improved healthcare operations and patient treatment activities. Real-time patient monitoring and remote diagnostics allow the physician to serve more patients and save human lives using internet of medical things (IoMT) technology. However, IoMT devices are prone to cyber attacks, and security and privacy have been a concern. The IoMT devices operate on low computing and low memory, and implementing security technology on IoMT devices is not feasible. In this article, we propose particle swarm optimization deep neural network (PSO-DNN) for implementing an effective and accurate intrusion detection system in IoMT. Our approach outperforms the state of the art with an accuracy of 96% to detect network intrusions using the combined network traffic and patient's sensing dataset. We also present an extensive analysis of using various Machine Learning(ML) and Deep Learning (DL) techniques for network intrusion detection in IoMT and confirm that DL models perform slightly better than ML models.

Keywords: internet of medical things; cyber security; intrusion detection system; particle swarm optimization; deep learning; deep neural network; network attacks

Citation: Chaganti, R.; Azrour, M.; Vinayakumar, R.; Naga, V.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. https://doi.org/10.3390/su141912828

Academic Editors: Amir Masoud Rahmani, Stavros Shiaeles, Firuz Kamalov and Seyedeh Yasaman Hosseini Mirmahaleh

Received: 15 September 2022
Accepted: 28 September 2022
Published: 8 October 2022

1. Introduction

The number of intelligent devices connected to the internet has been growing daily. According to Gartner, the number of connected Internet of Things(IoT) devices is predicted to be 27 billionby 2025, which is almost double the number of IoT devices connected to the Internet in 2021 [1]. The integration of intelligence capabilities into medical devices revolutionizes the medical field. The IoT integration with medical devices is termed as internet of medical things (IoMT). IoMT devices almost cover 30% of the IoT device market [2]. IoT technology's adoption in the medical field has improved patient health monitoring, healthcare operations, and remote healthcare services. However, security and privacy have been a concern in technology-enabled healthcare operations. For instance, as per the Cynerio report [3], more than half of the medical devices connected to the IoT contain critical vulnerabilities. The unintended exposure of these devices in public may pose security risks and help the adversaries to leverage the critical vulnerabilities. Attackers may use the advanced persistent threats (APT) and known vulnerabilities to compromise the victim devices [4]. Successful exploitation of the vulnerabilities may impact healthcare operations and put human life in danger. So, security should be considered a high priority in remote health monitoring using IoMT [5–8].

The attack detection and mitigation in IoMT can be performed using various techniques and methodologies. Various attacks, such as man in the middle, malicious network traffic injection, and denial of service, are performed to attack and compromise the IoMT networks. Some detection and prevention techniques include log monitoring, vulnerability management, threat intelligence, end device monitoring, intrusion detection, and prevention systems. The intrusion detection system is a commonly used technique to identify security issues and network attacks in IoMT. The network traffic anomalies, signature-based rules, or security policies are implemented in the intrusion detection system (IDS) to identify the network attacks in the IoT-enabled networks [9]. These traditional security detection techniques are ineffective, as the attacker constantly updates attack strategies and uses advanced hacking techniques. For instance, the security policies can be easily evaded if the attacker performs network reconnaissance and reverse engineering the network devices, such as router and firewall configurations. Researchers have started exploring machine learning (ML) and deep learning (DL) solutions to improve attack detection. The emergence of computing and processing capabilities allows us to use the ML and DL techniques at scale and predict the attack events accurately.

Intelligent IDS solutions have been proposed in the literature to detect the attacks in conventional networks using ML and DL techniques [10]. However, these solutions are not applicable in the IoMT context because various health IoT sensors connected to the internet and the conventional network datasets are not ideal for evaluating attack detection in IoMT. Moreover, in smart health applications, most of the existing works focus on only analyzing the network traffic to identify the IoMT attacks [10–13]. In an application like IoMT, patient biometric information is important and gives more insights into the patient's condition. There is a direct relationship between sudden drops in the patient sensing data and the attacks impacting the network to influence the confidentiality, availability, and integrity of healthcare data. So, we considered the combined network traffic and patient biometrics dataset to predict the attack events and analyze the relationship between the two disparate data types when the attack events occur.

Hady et al. [14] utilized the combination of the network traffic data and patient sensing data as a dataset and showed that the combined dataset slightly improved the attack detection performance. Nevertheless, the detection performance can still be improved. Ref. [15] augmented the dataset by making the normal and attack data equal in proportion. This work did not consider the network to attack traffic proportion in a real-time network traffic scenario. To improve the attack detection performance and ensure that the dataset follows the real-time attack traffic proportions, we preprocess the datasets, apply the feature selection technique PSO and utilize various ML and DL models to study the accurate prediction of IoMT attacks. In the end, our main contributions to this work are as follows.

- Propose particle swarm optimization deep neural network based (PSO-DNN) model to effectively detect IoMT attacks using the network traffic and patient biometric combined datasets.
- Perform detailed detection performance analysis of various machine learning and deep learning models to improve the IoMT intrusion detection system attack detection.
- Obtain better performance compared to the state-of-the-art works reported on the same datasets with an accuracy of 96%.

The remainder of the paper is described as follows. Section 2 discusses the background and related work related to the proposed work. Section 3 describes the proposed approach to improve intrusion detection in IoMT. Section 4 describes the dataset used in our study. Section 5 discusses the experimental setup and performance evaluation of ML and DL models used in our study. Section 6 includes the discussion and future work on the IoMT intrusion detection system. Section 7 concludes the paper.

2. Background and Related Work

In this section, the state-of-the-art work related to cyber attack detection using machine learning and deep learning techniques in IoMT is discussed, and we also discuss the limitations in the related work.

The IoMT network comprises the IoT medical devices connected to the patient's body or patient premises, an IoT gateway to connect with the conventional network, and the internet to monitor the patient's health condition and patient activity remotely. A successful attack on the IoMT network can have significant consequences, including patient life. Several works have been proposed in the literature to detect and mitigate cyber attacks in the IoMT network. The signature and anomaly-based intrusion detection system has existed for decades to detect attacks, including in the IoMT networks. However, the signature/policy-based solutions will not be able to identify the novel attacks, including advanced persistent threats. Although the anomaly-based solution is able to detect unknown attacks, the false positive rate is much higher in anomaly solutions. Additionally, tuning is required to set the thresholds and flag the attacks.

Recently, machine learning techniques have been proposed in the literature for intrusion detection in IoMT networks [16–18] and other technology fields [19]. The authors in [20] surveyed the security and privacy solutions in IoMT and discussed various solutions, including machine learning solutions to solve the attack detection problem. The authors concluded that an effective intrusion detection system still needs to be proposed to detect the attacks proactively, as the IoT devices are memory- and computationally scarce, and little security control implementation is performed at the device level.

In [16], the authors proposed an ensemble classifier-based intrusion detection system to classify attacks in smart hospitals. The bagging decision tree techniques obtained 93.2% accuracy in classifying the attacks in the KDDcup-99 dataset. It is also important to mention that the KDDcup-99 datasets were generated in the conventional network environment long ago, and the IoT device traffic is not included in the dataset simulation. Moreover, the classification accuracy can be improved to an extent on the KDD datasets. The authors in [17] presented an ensemble of the decision tree, naive Bayes, and random forest in the first stage. XGBoost was used in the second stage to classify the normal and attack network records. The IoT-based dataset ToN-IoT was used to perform the experiments and evaluate their proposed model. The reports show that their model obtained 96.35% accuracy in classifying the attacks in IoMT. However, the ToN_IoT dataset was generated in the industrial IoT network setup, and the Modbus weather sensors were used to generate the IoT data. These two sensors are not generally used in the IoMT environment. So, the reported results may not be applicable for detecting IoMT network attacks.

Radoglou et al. [11] explored the active learning approach to retrain the ML models and tested the proposed approach in HTTP and Modbus communication protocol network datasets. The CIC-IDS2017 dataset was used to test the performance of ML models using an active learning approach on HTTP communication protocol network datasets. The authors reported that the decision tree classifier achieved 96.44% accuracy in classifying the attacks. On the other hand, for the Modbus datasets, random forest obtained 94.45% accuracy. zachos et al. [21] combined the network traffic feature, IoT device feature, and gateways features to form a unique feature set and applied machine learning models to improve the performance of the attack detection in the IoMT network. The CPU and memory consumption level features in the IoT device were considered for evaluation. The authors showed that the random forest performed better than other ML models for attack detection in IoMT. Thamilarasu et al. [22] proposed a mobile agent-based intrusion detection to detect network and device-based attacks in IoMT. The machine learning and regression algorithms were used to test the simulation-generated datasets. Accuracies of 99.8% and 97.93% were obtained for network level and device level intrusion detection, respectively, when the ML model DT was used for evaluation. Binbusayyis et al. [23] evaluated the performance of the ML algorithm in the Bot-IoT dataset. The Bot-IoT dataset covers the Denial of service (DoS), Distributed Denial of Service (DDoS), scan, and theft

attack categories. However, IoMT-based attacks, such as man in the middle attacks and spoofing attacks, are not included in the dataset. The authors reported that the decision tree achieved 100% accuracy on the test dataset and obtained more than 99% with other ML models, such as KNN, NB, and SVM.

Overall, the ML-based models used to perform the attack detection in the IoMT environment indicate that most datasets were not generated, focusing on the IoMT attacks and the IoMT environment. However, the reported results were impressive, with an accuracy of more than 95% in most of the contributions. The input features may include network traffic, metric feature, IoT device memory, or CPU features for the IoMT study. None of the above works considered patient biometric data as a feature to detect cyber attacks in IoMT.

Some researchers also explored the deep learning models to detect or classify the attacks in the IoMT network. The authors in [12] applied particle swarm optimization (PSO) for feature selection and then used ML/DL-based models to detect cyber attacks in the IoMT. The authors considered the NSL-KDD datasets to evaluate the performance of the proposed approach. The PSO and RF-based solution obtained the best results with an accuracy of 99.76%. However, the dataset NSL-KDD was not generated focusing on the IoT network environment and is not the right dataset to evaluate attack detection in IoMT networks. Awotunde et al. [24] utilized a deep feed-forward neural network to classify the network attacks in the IoT network. The deep autoencoder was used to reduce the feature dimension. The network flow records were extracted from the dataset ToN-IoT to conduct the experiments. The authors reported that their model DAE-DFFNN obtained 89% accuracy and mentioned that it performed better than ML models like SVM and DT. The authors in [25] proposed an SDN-enabled CNN and LSTM hybrid DL model framework for IoMT malware detection. The authors obtained more than 99 percent accuracy in detecting malware. However, the proposed method was not evaluated for the IoMT intrusion detection system to detect network attacks in IoMT. The authors in [13] leveraged an intelligent agent-based swarm neural network for intrusion detection in IoMT. The ToN-IoT dataset is used to conduct the experiments, and it reported that their proposed neural network obtained 99.5% accuracy on the ToN-IoT dataset. Manimurugan et al. [26] presented a deep belief neural network to classify the network attacks in the IoMT. A CICIDS dataset was considered to evaluate the proposed method. The deep belief neural network reported more than 96% accuracy for attack classification. However, the CICIDS dataset was not generated focusing on the IoMT network attacks.

The review of DL models used for IoMT intrusion detection indicates that DL models are not highly leveraged to detect the IoMT network attacks except swarm-based neural networks. Additionally, the literature-reviewed DL models only consider the network traffic pr metric datasets to classify or detect the attacks. The patient bio-metric data are not considered a feature in any of the above-discussed works. Table 1 compares the ML- and DL-based state-of-the-art solutions for attack detection in IoMT.

Table 1. State-of-the-art attack detection in IoMT using ML and DL techniques.

Article	Dataset	ML/DL Technique	Accuracy	Limitation
[11]	CIC-IDS2017	RF	94.45%	Only network traffic features, CIC-IDS2017 not focused on IoMT network
[12]	NSL-KDD	PSO-RF	99.76%	Dataset is not applicable for IoMT attacks, only network traffic data
[13]	ToN-IoT	Swarm neural network	99%	Only network traffic data
[25]	-	CNN-LSTM	99%	Only for malware attack detection
[16]	KDDCup-99	Ensemble Classifiers	93%	Dataset not related to IoMT, only network traffic considered
[26]	CICIDS	Deep belief neural network	96%	The dataset is not related to IoMT, only network traffic
[24]	NF-ToN-IoT	Swarm neural network	89%	Low accuracy
[23]	Bot-IoT		99%	Only network traffic in the dataset
[17]	ToN-IoT	Ensemble Classifier	96.35%	Performance improvement, only network traffic

Related Work

Our literature survey indicates that only two research works recently considered the network traffic and patient bio-metric data as features for IoMT attack detection. Hady et al. [14] created a healthcare monitoring system testbed and generated the datasets simulating the network attacks. The dataset contains the network traffic and the patient's biometrics data for analysis. The authors showed that the combination of the network traffic and the patient biometrics data improves the attack detection performance compared to considering only network traffic. The reported results showed detection performance of approximately 90% accuracy when machine learning techniques were applied. However, the work did not explore the usage of efficient data analytics methods to improve detection performance. The authors in [15] utilized a tree classifier model with data preprocessing, and data augmentation methods to improve the performance on the same datasets used by [14]. The authors made the balanced normal and attack traffic datasets using data augmentation techniques. The data augmentation results in an overfitting problem. Additionally, the network traffic always contains the majority of the normal traffic and a minority of attack traffic. So, the consideration of imbalance traffic is the best-opted characteristic to mimic the real-time network traffic and test the detection performance of the ML models. We were inspired to improve the performance of attack detection in IoMT by selecting the best features from both the network traffic and patient bio-metric features and applying the computer network domain knowledge to consider the real-time network traffic attack versus normal traffic proportions. Instead of augmenting the dataset, we considered the practical normal and attack traffic proportion datasets and evaluated the performance of IoMT attack detection.

3. Proposed Approach

To effectively identify the IoMT attacks using network traffic and patient biometric data, we explored various ways to improve the attack detection performance. Prior to discussing our proposed approach, we describe the IoMT intrusion detection system architecture. Figure 1 displays a typical IoMT network architecture used to manage security operations and predict the attacks using ML or DL techniques. The IoMT intrusion detection system architecture contains patient sensor devices, IoT gateway, network traffic collector, ML/DL data processing pipeline, intrusion detection system, and the security operators to monitor the attacks. The sensor devices may include a temperature sensor, pulse rate detector, heart rate detector, ECG device, blood pressure, and respiration rate monitoring device, but are not limited to these. IoT network protocols, such as MQ Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP), are used to send the IoT sensing device's information to the remote servers. The IoT gateways collect the sensor data through wireless or wired communication and send the data to remote locations. The network traffic as well as the patient biometrics data are collected in our approach.

The intrusion detection system mentioned in Figure 1 includes the data processing and analytical capabilities to detect intrusion in the IoMT network. Continuous monitoring and analysis are required at the intrusion detection system level to tune the alerts and reduce the false positives. The applications of the IoMT system include remote patient monitoring and monitoring of the physical premises in the hospital environment to save and cure the patient health.

Figure 2 shows our proposed approach to improve the IoMT attack detection performance using ML and DL models. In contrast to performing the network traffic analytics and detecting intrusion in the network infrastructure, we leverage the IoT sensing data from the patient-specific IoMT systems to identify the patient biometrics anomalies and improve the overall attack detection performance when an adversary conducts attacks in the IoMT network infrastructure. The network traffic and patient biometric data are combined using the timestamp of the network traffic events and patient biometric data events in the IoMT. The final dataset includes the majority of the network traffic features and a minority of the patient biometric features.

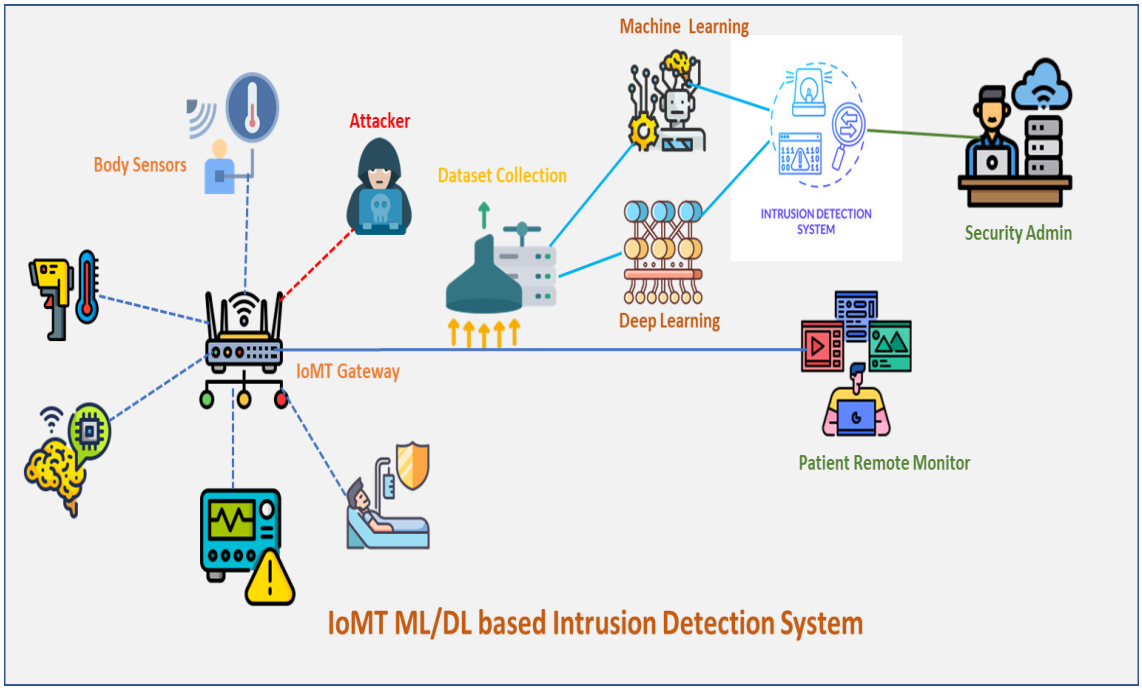

Figure 1. IoMT ML- and DL-based intrusion detection system.

Data Preprocessing: The data were preprocessed using the simple imputer and standard-scalar technique. In the simple imputer, the missing values in the column are replaced with either mean, median, or most frequent values in the same column. We used the median statistic to replace the missing values in the feature columns. Standard scalar: Standard scalar is one of the well-known data standardization techniques. The feature data are standardized by subtracting the value from the mean of the feature values and dividing it by the standard deviation of the feature data. It will result in the feature data being normally distributed with mean zero and unit variance.

PSO Feature Selection: The selection of relevant features is needed to improve the accuracy and perform the prediction faster of the model. We use the particle swarm optimization technique [27] to select the relevant features for IoMT attack prediction. Let $f_1, f_2, f_3 \ldots\ldots\ldots f_d$ be the d features of the dataset. The selection of the features is represented as 1. If the feature is not selected, it is assigned as 0.

$$f = [f_1, f_2, f_3 \ldots\ldots\ldots f_d], f_i \in [0, 1] \quad (1)$$

The total number of features in the dataset is considered '*d*'. In order to select the feature, we assign a threshold value of 0.5. If the feature value is greater than the threshold value of 0.5, then the feature will be selected. Otherwise, the feature value will be 0.

$$f_i = \begin{cases} 1 & f_i \geq 1 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

The function F(..) will optimize the classification accuracy by penalizing the number of features selected. The objective is to minimize the function F(...) in which the α represents a parameter to decide the trade-off between classification accuracy and the number of features selected with respect to the total number of features. The parameter P is denoted as the classification accuracy. $N_{Selected}$ denotes the number of the selected features, and $N_{Featured}$ denotes the total number of features [27].

$$F(f) = \alpha \times (1 - P) + (1 - \alpha) \times \frac{N_{Selected}}{N_{Featured}} \tag{3}$$

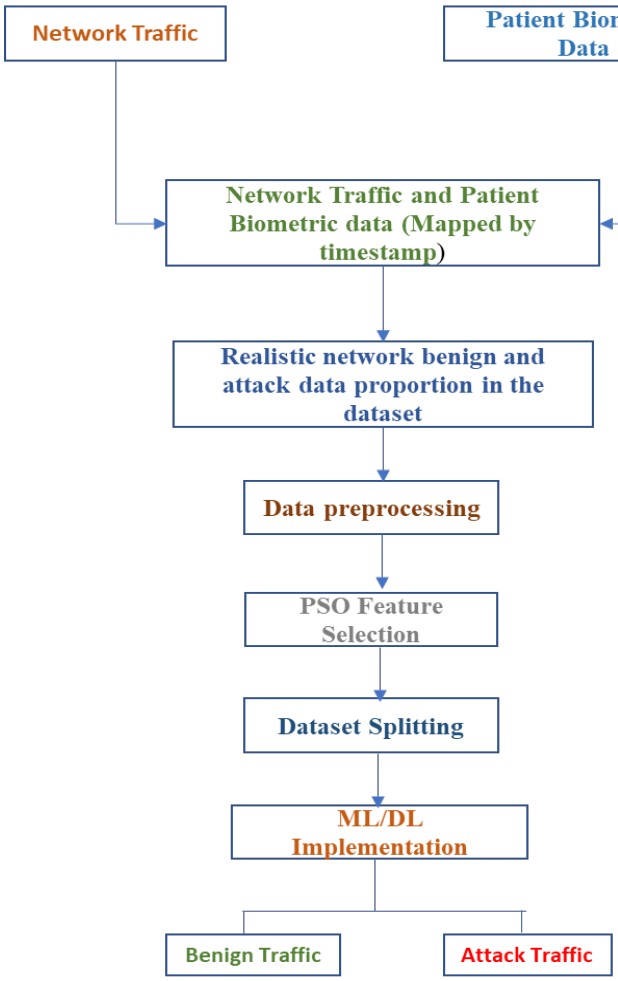

Figure 2. Our Approach to detect IoMT attacks

Figure 3 shows the fitness values for the PSO when the number of iterations is varied from 0 to 100. We obtained the 8 optimal features out of the network and biometric combined 43 features during the feature selection process. As the number of features reaches 8, the fitness value becomes constant and maintained well below the 0.231 fitness value. So, we used the PSO-based features to evaluate the IoMT attack detection performance.

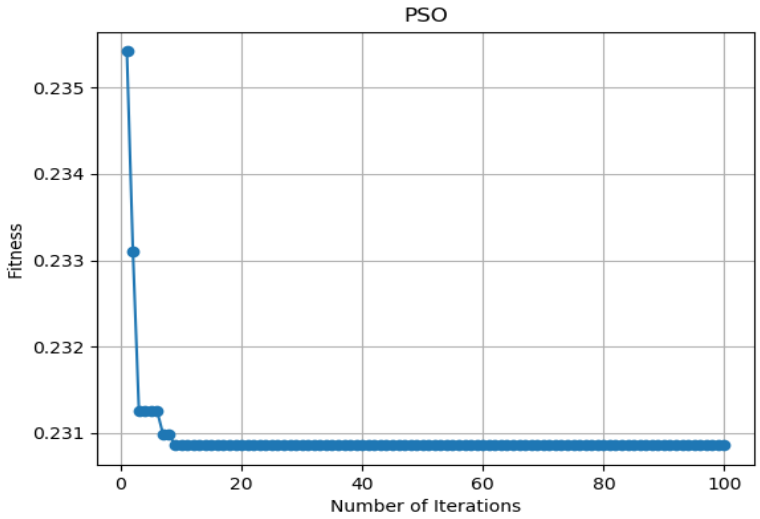

Figure 3. PSO: fitness versus the number of iterations.

The dataset is split into training and test datasets to conduct the experiments and evaluate the performance. We split the dataset into 70% training data and 30% test data for our experimental evaluation. The following ML and DL algorithms are used to test our datasets and determine the best-performing models when the network traffic data and patient biometric data are combined.

3.1. Machine Learning Models

3.1.1. Logistic Regression (LR)

Logistic regression is used for the binary classification of a given dataset. The logistic regression takes the real values as input and predicts the probability of the input features associated with the output class. The coefficient values are determined using stochastic gradient descent. A logistic function is used to transform the output as the probability.

The probability of predicting the class R, given the input sample X_i is defined as

$$Pr(Y_i = R) = \frac{e^{\beta_r . X_i}}{\Sigma_{0 \le c \le R} e^{\beta_c . X_i}} \quad (4)$$

3.1.2. K-Nearest Neighbor (KNN)

KNN can be used for both classification and prediction. The prediction works based on feature similarity. The nearest neighbors are selected based on different distance measures. We used the uniform weight to assign equal weights to all neighbors. The number of neighbors is selected as 3 in our evaluation, and the average nearest neighbor data values are assigned as the final predicted values. The Euclidean distance (E) is used to determine the nearest neighbors [28].

$$E = \sqrt{\sum_{i=1}^{k} (x_i - y_i)^2} \quad (5)$$

where k denotes the number of neighbors, and x_i and y_i are the data points in the ith dimension.

3.1.3. Decision Tree

A decision tree is a tree-like graph that is used for regression and classification problems. Each node or branch in the tree represents the feature of a dataset. The entropy and the information gain against each feature against the target variable used to construct the DT. The test data class is predicted by traversing through the tree up to the leaf nodes.

3.1.4. AdaBoost

Adaptive boosting is one of the well-known boosting techniques used to improve weak classifiers' performance. The multiple weak classifiers are combined to form a robust classifier using boosting techniques like Adaboost. A single classifier may not accurately classify the input. So, the misclassified classes are passed through another classifier to improve the overall accuracy. The classifiers can be decision trees, logistic regression, random forest, etc.

3.1.5. Random Forest (RF)

RF is a family of decision tree-based machine learning algorithms. Ensemble learning is used to perform the classification and predictions, and bootstrapping RF is used to perform the predictions in this work. The bootstrapping method combines ensemble learning and the random selection of the decision trees to determine the prediction output as the average value of all the decision tree predictions.

Let $b = 1$ to B is the number of decision trees, $\hat{C}_b(x)$ denotes the regression prediction value of the bth decision tree [29], then the regression prediction of the RF forest is defined as

$$\hat{C}_{rf}^{B}(x) = Average\{\hat{C}_b(x)\}_1^B \tag{6}$$

3.1.6. Support Vector Machine (SVM)

SVM is a supervised machine learning algorithm used for regression and classification problems. SVM separates the data of two classes with a hyperplane or decision boundary. We selected "linear kernel" in our experiments to classify benign and attack traffic in the IoMT network. The original feature space is converted into a new feature space to support the nonlinear decision boundaries.

The hyperplane function is denoted as

$$H(x) = \begin{cases} +1, & \text{if } w.x + b \geq 1 \\ -1, & \text{if } w.x + b \leq 1 \end{cases}$$

The objective function needs to be minimized such that $y_i(w.xi+)b \geq 1$ is satisfied all the time.

3.2. DL Methods

3.2.1. Deep Neural Networks (DNN)

A deep neural network contains more than two hidden layers, the input layer, and the output layer. DNN contains more than one multi-layer perception layer to produce the output. MLP is a global approximator and well suited for mapping the non-linear input–output combination. Typically, MLPs consist of three layers. The input layer feeds the input values to the neural network. The output layer performs the classification or prediction of the given problem. The hidden layer includes the neurons and supports the computations to process the input data and forward the processed data as input to the output layer. The number of hidden layers can be arbitrary. The neuron processing unit is represented as follows: [30].

$$f(x) = \Phi(\sum_{i=1}^{m} w_i * x_i) + b \tag{7}$$

where b denotes the bias value, W_i denotes the ith neuron weight and the x_i denotes the input to the ith neuron unit. Φ is the non-linear activation function, and $f(x)$ is the neuron processing unit output.

3.2.2. Convolutional Neural Network (CNN)

A convolutional neural network is a feed-forward neural network that takes input in a one-dimensional or two-dimensional form. CNN is commonly used for image classification

and object detection in images. The CNN contains a convolutional layer, *RelU* layer, pooling layer, and fully connected layer. The convolution layer extracts the feature patterns from the input features, and *Relu* incorporates the non-linearity into the network. The pooling layer reduces the dimensionality of the feature map. Finally, the fully connected layer multiplies the input with weights and adds bias values to produce the output. Usually, the last layer of the CNN is a fully connected layer.

3.2.3. Long Short-Term Memory LSTM

LSTM is a class of recurrent neural networks (RNN). LSTM is used to predict and classify the time series input data. In contrast to the RNN, LSTM remembers the long-term dependencies of the input data. LSTM comprises the input gate, forget gate, and output gate. The first gate determines whether or not the information from the previous timestamp data is valuable. The second gate is used to learn the input data, and the third gate passes the information to the next timestamp.

4. Dataset Description

In this section, the IoMT dataset considered to perform the data model evaluation is discussed in detail. The dataset was created using a real-time health monitoring testbed [14]. The testbed comprises the sensor devices attached to the patient's body, the network gateway, and the Software Defined Network (SDN) controller for visualizing the network traffic. The network traffic and sensor data generated in the testbed are used to detect the anomalies in the data and identify the attacks. Three attacks were simulated in the environment to generate the attack dataset. Those attacks are man-in-the-middle attacks, data injection, and spoofing attacks.

The man-in-the-middle attack includes the attacker who joins the patient health monitoring system and can read/manipulate the network traffic on the fly. This attack results in violations of the patient's data confidentiality and integrity in the network. The data injection attack includes manipulating the patient health network packets passing through the gateway. This attack results in violating patient data integrity. The spoofing attacks result in reading the network traffic passing through the gateway. It violates the patient's data confidentiality.

The network traffic and patients bio-metric data combined dataset is generated using the ARGUS tool [31]. The biometric data includes the temperature, peripheral oxygen saturation, pulse rate, systolic blood pressure, diastolic blood pressure, heart rate, respiration rate, and ECG ST segment data. The network traffic flow records and their metrics are captured to obtain the overall network traffic features. Overall, the dataset contains 44 features, including 35 network traffic features out of 44 features. The dataset output is labeled as an attack or normal traffic. The attack traffic is labeled as "0", whereas the normal traffic is labeled as "1". Table 2 shows all the features considered in the dataset and the description of each feature and the feature type.

Table 2. Dataset Features.

Metric	Description	Type
	ML Features	
SrcBytes	Source bytes in the flow record	Flow metric
DstBytes	Destination bytes in the flow record	Flow metric
SrcLoad	Source load (bitspersecond)	Flow metric
DstLoad	Destination load (bitspersecond)	Flow metric
SreGap	Source bytes missing in data	Flow metric
DstGap	Destination bytes missing in data	Flow metric
SIntPkt	Source inter packet arrival time	Flow metric
DIntPkt	Destination inter packet arrival time	Flow metric

Table 2. *Cont.*

Metric	Description	Type
	ML Features	
SIntPktAct	Source active inter packet arrival time	Flow metric
DIntPktAct	Destination active inter packet arrival time	Flow metric
SrcJitter	Source jitter	Flow metric
DstJitter	Destination jitter	Flow metric
sMaxPktSz	Source maximum transmitted packet size	Flow metric
dMaxPktSz	Destination maximum transmitted packet size	Flow metric
sMinPktSz	Source minimum transmitted packet size	Flow metric
dMinPktSz	Destination minimum transmitted packet size	Flow metric
Dur	Duration	Flow metric
Trans	Aggregated packets count	Flow metric
TotPkts	Total packets count	Flow metric
TotBytes	Total packets bytes	Flow metric
Loss	Retransmitted or dropped packets	Flow metric
pLoss	Percentage of retransmitted or dropped packets	Flow metric
pSrcLoss	Percentage of source retransmitted or dropped packets	Flow metric
pDstLoss	Percentage of destination retransmitted or dropped packets	Flow metric
Rate	Number of packets per second	Flow metric
Load	Load	Flow metric
Temp	Temperature	Biometric
SpO2	Peripheral oxygen saturation	Biometric
Pulse_Rate	Pulse rate	Biometric
SYS	Systolic blood pressure	Biometric
DIA	Diastolic blood pressure	Biometric
Heart_Rate	Heart rate	Biometric
Resp_Rate	Respiration rate	Biometric
ST	ECG ST segment	Biometric

As shown in Table 3, the dataset comprises the 14,272 normal and 2046 attack sample network records. We randomly selected 1400 attack samples to balance the attack and normal traffic proportions in the dataset. In real-time networks, the attacks are rarely seen, and the normal-to-attack traffic ratio is very high. To mimic the real-time scenario, we deduced the attack sample count in the dataset and considered an unbalanced dataset for performance evaluation.

Table 3. IoMT network traffic and patient biometrics dataset.

Dataset	Raw Data		Random Selection	
	Normal	Attack	Normal	Attack
IoMT Dataset	14,272	2046	14,000	1400

5. Experimental Evaluation and Performance Comparison

In this section, we discuss the experimental setup and the performance evaluation of the ML and DL models used in our study. We also compare the performance of our approach with state-of-the-art IoMT solutions.

5.1. Software and Hardware Preliminaries

The experiments were performed on a virtual machine 64-bit Ubuntu operating system. The LTS 20.04 version was used for the operating system. The virtual machine is configured with 4GB RAM memory and Intel Core i5-4210U CPU@1.70GHz. The libraries scikit-learn (https://scikit-learn.org/stable/ 15 March 2022) and Keras (https://keras.io/ 15 March 2022) in Python were used to train and test the ML and DL models.

5.2. Evaluation Metrics

The performance evaluation of the models is measured using statistical parameters. We considered the commonly used four metrics for IoMT attack classification performance evaluation: true positive (TP), true negative (TN), false positive (FP), and false negative (FN) are used to define the metrics.

Accuracy is defined as the correct prediction of the traffic classification (both benign and attack) to the total prediction of the network traffic test data.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

Precision is defined as the correct classification of the attack network traffic to the sum of the correct classification of the attack traffic and incorrect classification of the attack traffic in the dataset. If the precision is high, then the model performs well.

$$Precision = \frac{TP}{TP + FP} \tag{9}$$

Recall is defined as the correct classification of the attack network traffic to the sum of the correct classification of the attack network traffic and the missed classification of the attack network traffic in the dataset.

$$Recall = \frac{TP}{TP + FN} \tag{10}$$

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

$$F1 - Score = \frac{2 * Recall * Precision}{Recall + Precision} \tag{11}$$

ML model performance: The ML techniques, such as logistic regression, KNN, decision tree, Adaboost, and random forest, are considered to detect the IoMT attack. As shown in Figure 4, the Adaboost technique performed better than the other models in IoMT attack binary classification. The decision tree is the least well performing, with an accuracy of 91.6%. The KNN and random forest obtained similar performance with accuracy better than the decision tree. Logistic regression and SVM performed better than all the models, except AdaBoost.

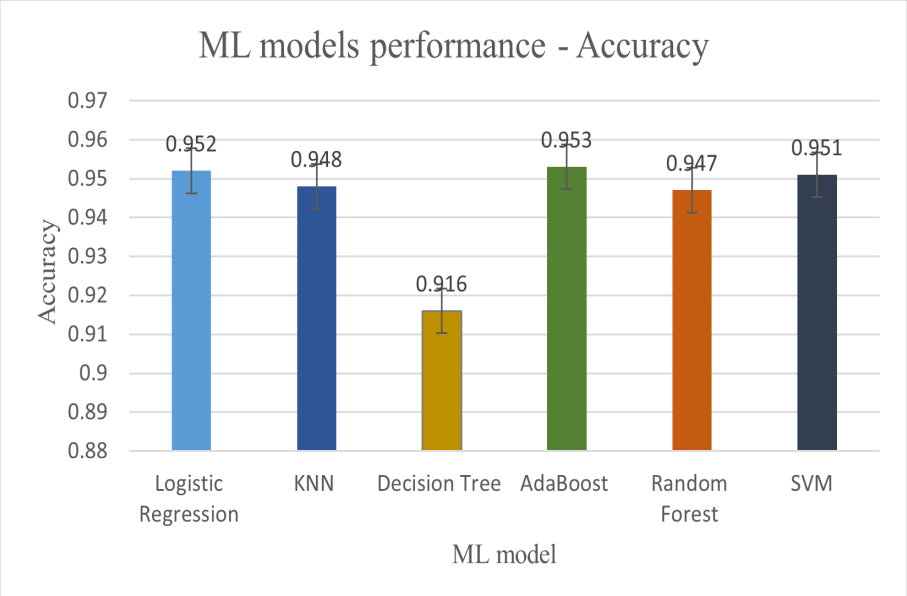

Figure 4. ML performance.

Table 4 presents the performance metrics precision, recall, and F1-score of the ML model to classify the IoMT traffic. The LR, SVM, and Adaboost obtained the best precision with a value of 0.95. All the models achieved the same recall except the decision tree. The F1-score metric is valuable for imbalanced dataset performance evaluation. Adaboost obtained the best F1-score 95% out of the models considered in our study.

Table 4. ML algorithms performance.

Ml Model	Precision	Recall	F1-Score
Logistic Regression	0.95	0.95	0.94
KNN	0.94	0.95	0.94
Decision Tree	0.92	0.92	0.92
AdaBoost	0.95	0.95	0.95
Random Forest	0.94	0.95	0.94
SVM	0.95	0.95	0.94

The deep learning model's training accuracy and loss are measured when the number of epochs varies from 1 to 100. Figure 5 describes the training accuracy and loss of the DNN model when the epochs vary from 1 to 100 and the number of layers increases from 1 to 4. Figure 5 clearly shows that increasing the number of layers during the training will have no impact on the performance accuracy. We can also see that loss is slightly reduced when the epoch reaches 100. Similarly, the accuracy slightly improved in detecting the attacks. However, within the first few epochs, the neural network learns the feature set and predicts stable accuracy.

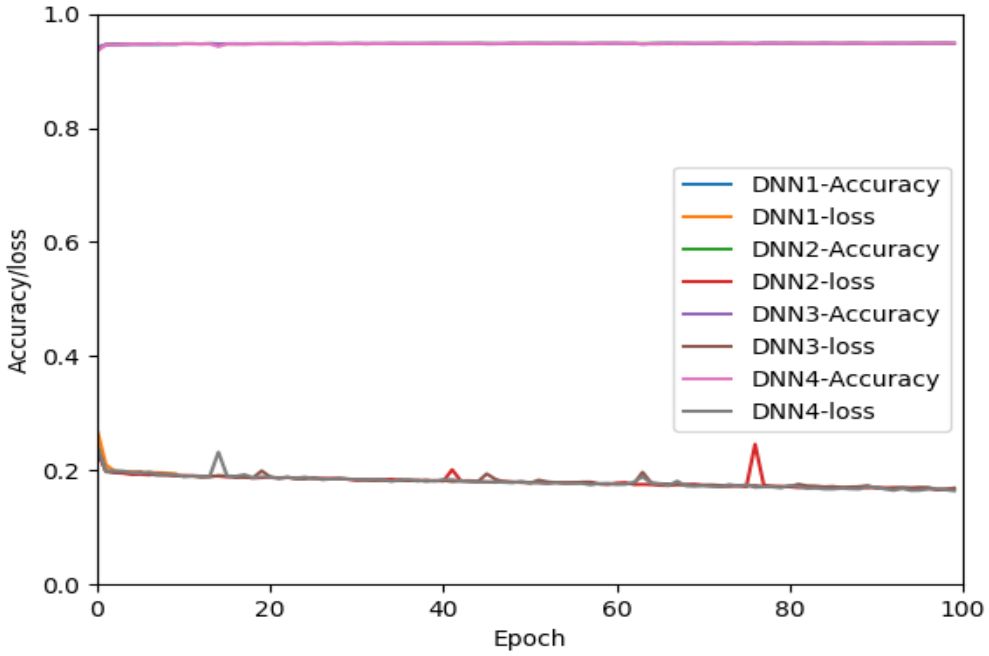

Figure 5. Accuracy and loss for DNN.

Figure 6 describes the training accuracy and loss for the CNN model when the epochs vary from 1 to 100. The CNN training accuracy and loss indicate that both the CNN and DNN show similar accuracy performance on the training dataset. We can see the training loss slightly drops when the epoch reaches 100.

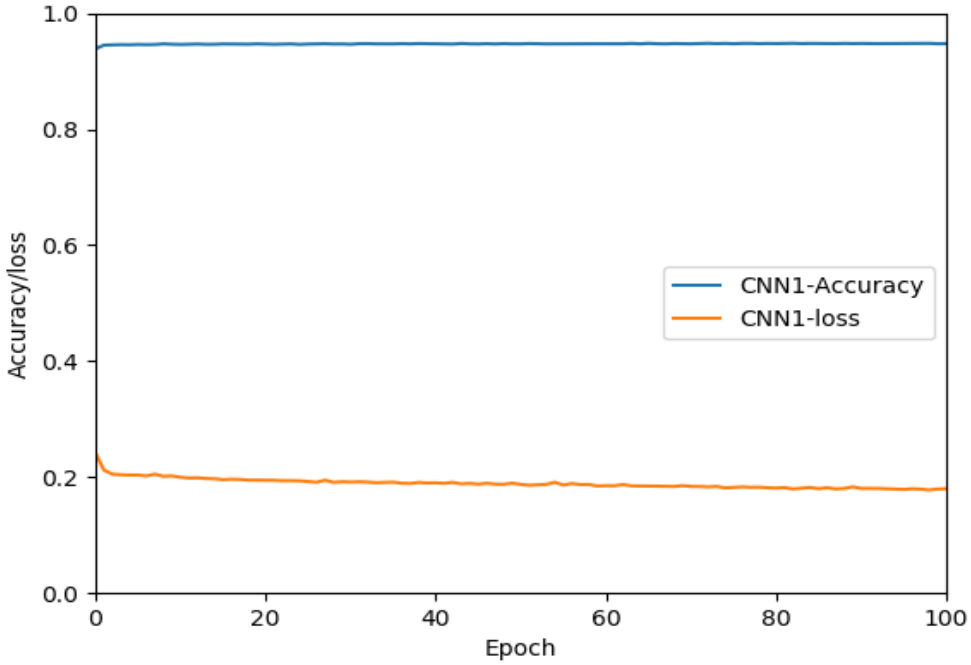

Figure 6. Accuracy and loss for CNN.

Figure 7 describes the performance of the training accuracy and loss of the LSTM when the epochs are varied from 1 to 100 and the number of LSTM layers is increased from 1 to 4. As the number of LSTM layers increases, the number of training losses decreases. We can clearly see the loss difference for LSTM 1 and LSTM 2 in Figure 7.

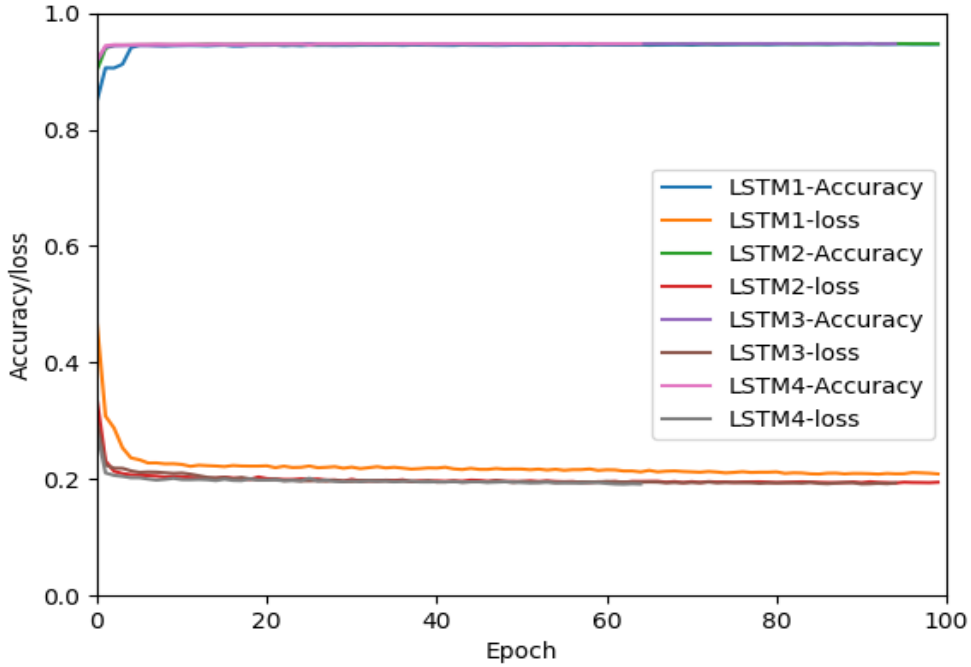

Figure 7. Accuracy and loss for LSTM.

We also evaluated the performance using DL models. Figure 8 shows the DL model performance accuracy. The DNN performed better than the CNN and LSTM models. As the number of layers increased from one to two in DNN, the performance was slightly increased in terms of accuracy. Overall, the DNN2 achieved the best accuracy compared to all the ML and DL models considered in our study.

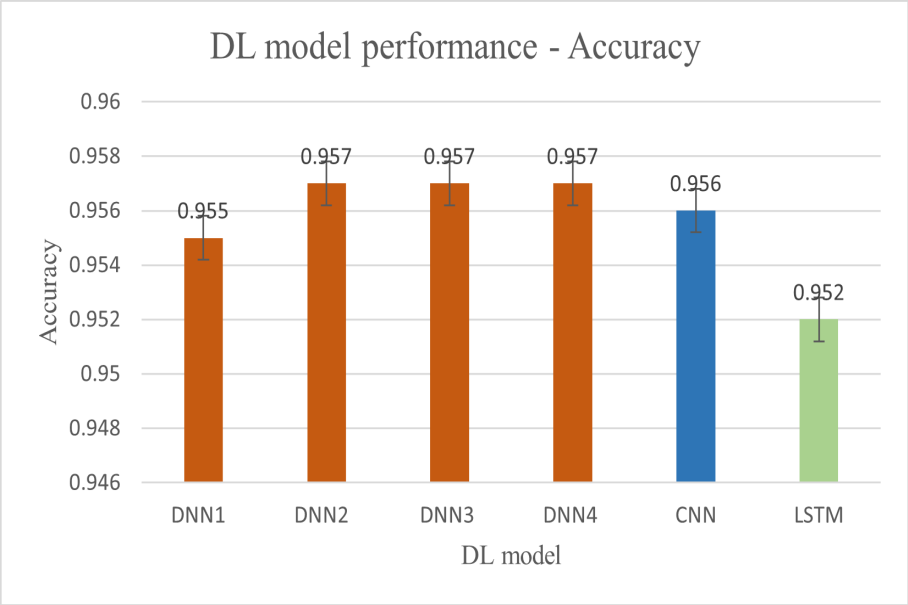

Figure 8. DL performance.

Table 5 represents the performance metrics of the DL models considered for our study. All the DL models, DNN, CNN, and LSTM, achieved the same precision. The DNN obtained a slightly good performance compared to the LSTM and CNN.

Table 5. DL algorithms performance.

DL Model	Precision	Recall	F1-Score
Logistic Regression	0.95	0.95	0.94
DNN1	0.96	0.96	0.95
DNN2	0.96	0.96	0.95
DNN3	0.96	0.96	0.95
DNN4	0.96	0.96	0.95
CNN	0.96	0.95	0.95
LSTM	0.96	0.95	0.95

5.3. Performance Comparison with Prior Art

As shown in Table 6, we compared the performance of our approach PSO-DNN with state-of-the-art solutions. The authors in [14] proposed KNN to detect the IoMT attacks when the network and patient biometric data were used. The authors did not explore the feature selection to select features. Moreover, the paper did not focus on the thorough analysis of the ML and DL models to detect the IoMT intrusion detection. Gupta et al. [15] improved the performance of the IoMT intrusion detection using data augmentation and the tree classifier technique. Data augmentation helped to have an equal proportion of the normal and attack data in the datasets. This is very unrealistic when it comes to real-time network attacks, and the proportion of the real and attack network traffic is high in real time. We proposed PSO feature selection and DNN model to improve the performance accuracy of the IoMT intrusion detection when the network traffic and patient biometric data are used as a dataset feature. We obtained 96% accuracy, which is a 3.2% improvement over the state-of-the-art work.

Table 6. Our work comparison with the prior art.

Article	ML Techniques	Accuracy	Advantages	Limitations
[14]	KNN	90%	Combined the patients biometric data and network traffic	Performance can be improved.
[15]	tree classifier	93%	Performance improved compared to [14]	Data augmentation results in unrealistic dataset. The attack traffic proportion in the network is very low.
Our work	PSO-DNN	96%	Improved performance and realistic	-

6. Discussion and Future Work

We leveraged PSO-based feature selection and the DNN model to predict the IoMT attacks. Although our work improved the performance of the IoMT intrusion detection, the dataset used for our evaluation mainly addresses the patient's confidentiality and integrity-based attacks. The denial of service attacks is not considered in our evaluation. One of our future works will be performing IoMT attack classification using ML and DL models, including the DoS, data injection, man-in-the-middle attacks, etc.

Data analytics plays a significant role in the smart health industry. The secured implementation of the machine learning operations (MLOps) is essential to align with the health industry regulations and maintain the compliance requirements. The combination of patient data with network data in our approach requires securely collecting, processing, and transforming the data in real-time applications. Hence, additional security measures are needed in MLops implementation to apply our approach in real-time healthcare industry applications.

Various sensing-related patient data are generated in the IoMT networks. The intrusion detection system deployment location and preserving the privacy of the patient data are important in the IoMT network. So, data anonymization techniques will be used in the future to preserve the privacy of the patients when collecting patient biometric data. The most relevant patient biometric features for attack detection will be studied to understand the correlation between attack detection and biometric feature.

We also want to explore the adversarial attacks in IoMT targeting the ML and DL solutions and manipulating the predictions. An adversary may compromise the machine learning operations infrastructure and poison the data. This results in attacks possibly going undetected, or new attacks being missed in the intrusion detection system.

7. Conclusions

In this article, we proposed the PSO feature selection method and DNN-based DL model to improve the performance of the intrusion detection system in IoMT. The combination of network traffic and patient biometric data dataset was considered to evaluate the performance of the proposed approach. Based on our study of ML and DL model performances, our proposed approach PSO-DNN performed better than other ML and DL models used in the prior art. We plan to extend our work to perform network attack classification and adversarial attacks detection [32] in IoMT.

Author Contributions: Conceptualization, R.C., N.V. and A.M.; data curation, R.C., A.D. and N.V.; formal analysis, R.C., V.R. and A.M. investigation, R.C., A.D. and N.V.; methodology, R.C., A.M., and V.R.; project administration, R.C., V.R. and B.B.; resources, R.C., V.R. and A.D.; software, R.C., N.V. and A.M.; supervision, R.C. and N.V.; validation, R.C., A.M. and V.R; visualization, R.C., A.D. and V.R.; writing—original draft, R.C. and B.B.; writing—review and editing, R.C. and B.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The dataset is available at https://www.cse.wustl.edu/~jain/ehms/index.html 15 March 2022.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hasan, M. Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally. 2022. Available online: https://iot-analytics.com/number-connected-iot-devices/ (accessed on 14 September 2022).
2. Cogniteq. Internet of Medical Things (IoMT): Innovative Future For Healthcare Cogniteq. 2022. Available online: https://www.cogniteq.com/blog/internet-medical-things-iomt-innovative-future-healthcare-industry (accessed on 14 September 2022).
3. Newman, L.H. Critical Bugs Expose Hundreds of Thousands of Medical Devices and ATMs WIRED. 2022. Available online: https://www.wired.com/story/access7-iot-vulnerabilities-medical-devices-atms/ (accessed on 29 August 2022).
4. Ren, Y.; Xiao, Y.; Zhou, Y.; Zhang, Z.; Tian, Z. CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution. *IEEE Trans. Knowl. Data Eng.* **2022**. [CrossRef]
5. Ahmad, R.; Alsmadi, I.; Alhamdani, W.; Tawalbeh, L. A comprehensive deep learning benchmark for IoT IDS. *Comput. Secur.* **2022**, *114*, 102588. [CrossRef]
6. Rbah, Y.; Mahfoudi, M.; Balboul, Y.; Fattah, M.; Mazer, S.; Elbekkali, M.; Bernoussi, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey. In Proceedings of the 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). IEEE, Meknes, Morocco, 3–4 March 2022; pp. 1–9.
7. Unal, D.; Bennbaia, S.; Catak, F.O. Machine learning for the security of healthcare systems based on Internet of Things and edge computing. In *Cybersecurity and Cognitive Science*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 299–320.
8. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
9. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
10. Ravi, V.; Alazab, M.; Selvaganapathy, S.; Chaganti, R. A Multi-View attention-based deep learning framework for malware detection in smart healthcare systems. *Comput. Commun.* **2022**, *195*, 73–81. [CrossRef]
11. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Lagkas, T.; Fragulis, G.; Sarigiannidis, A. A self-learning approach for detecting intrusions in healthcare systems. In Proceedings of the ICC 2021-IEEE International Conference on Communications. IEEE, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
12. Saheed, Y.K.; Arowolo, M.O. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEE Access* **2021**, *9*, 161546–161554. [CrossRef]
13. Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1969–1976. [CrossRef] [PubMed]
14. Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access* **2020**, *8*, 106576–106584. [CrossRef]
15. Gupta, K.; Sharma, D.K.; Gupta, K.D.; Kumar, A. A tree classifier based network intrusion detection model for Internet of Medical Things. *Comput. Electr. Eng.* **2022**, *102*, 108158. [CrossRef]
16. Saba, T. Intrusion detection in smart city hospitals using ensemble classifiers. In Proceedings of the 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 14–17 December 2020; pp. 418–422.
17. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Comput. Commun.* **2021**, *166*, 110–124. [CrossRef]
18. Chaganti, R.; Varadarajan, V.; Gorantla, V.S.; Gadekallu, T.R.; Ravi, V. Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet* **2022**, *14*, 250. [CrossRef]
19. Li, M.; Liu, Y.; Tian, Z.; Shan, C. Privacy Protection Method Based on Multidimensional Feature Fusion Under 6G Networks. *IEEE Trans. Netw. Sci. Eng.* **2022**. [CrossRef]
20. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
21. Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C.; Rodriguez, J. An anomaly-based intrusion detection system for internet of medical things networks. *Electronics* **2021**, *10*, 2562. [CrossRef]
22. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
23. Binbusayyis, A.; Alaskar, H.; Vaiyapuri, T.; Dinesh, M. An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. *J. Supercomput.* **2022**, *78*, 17403–17422. [CrossRef] [PubMed]
24. Awotunde, J.B.; Abiodun, K.M.; Adeniyi, E.A.; Folorunso, S.O.; Jimoh, R.G. A deep learning-based intrusion detection technique for a secured IoMT system. In Proceedings of the International Conference on Informatics and Intelligent Applications, Ota, Nigeria, 25–27 November 2021; pp. 50–62.

25. Khan, S.; Akhunzada, A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). *Comput. Commun.* **2021**, *170*, 209–216. [CrossRef]
26. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
27. Poli, R.; Kennedy, J.; Blackwell, T. Particle swarm optimization. *Swarm Intell.* **2007**, *1*, 33–57. [CrossRef]
28. Guo, G.; Wang, H.; Bell, D.; Bi, Y.; Greer, K. KNN model-based approach in classification. In Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Rhodes, Greece, 21–25 October 2003; pp. 986–996.
29. Oshiro, T.M.; Perez, P.S.; Baranauskas, J.A. How many trees in a random forest? In Proceedings of the International Workshop on Machine Learning and Data Mining in Pattern Recognition, Berlin, Germany, 13–20 July 2012; pp. 154–168.
30. Noriega, L. *Multilayer Perceptron Tutorial*; School of Computing. Staffordshire University: Stoke-on-Trent, UK, 2005.
31. Argus. Openargus-Home. Available online: https://openargus.org/ (accessed on 13 September 2022).
32. Jiang, H.; Lin, J.; Kang, H. FGMD: A robust detector against adversarial attacks in the IoT network. *Future Gener. Comput. Syst.* **2022**, *132*, 194–210. [CrossRef]