Efficient Intrusion Detection using OptCNN-LSTM Model based on hybrid Correlation-based Feature Selection in IoMT

Sultan Almotairi[1,*], Deepak Dasaratha Rao[2], Olayan Alharbi[3], Zaid Alzaid[4], Yasser M. Hausawi[5], Jaber Almutairi[6]

[1] Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
[2]Indian Institute of Technology, Patna, Bihar, India

[3] Department of Information Systems, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia

[4] Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah, Medinah, 42351, Saudi Arabia
[5] IT Programs Center, Faculty of IT Department, Institute of Public Administration, Riyadh, 11141, Saudi Arabia
[6] Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
Emails: almotairi@mu.edu.sa; deepakrao@ieee.org, o.alharbi@mu.edu.sa; zsalzaid@iu.edu.sa; Hawsawiy@ipa.edu.sa; jalmutairi@taibahu.edu.sa
Corresponding Author: Sultan Almotairi, almotairi@mu.edu.sa

Abstract

Intrusion detection in the IoMT (Internet of Medical Things) represents the process of keeping track of and discovering unauthorized or malicious actions in medical devices and networks. Some of its benefits include early detection of potential threats, prevention of data breaches, and protection of patient privacy. Aside from these benefits, some difficulties are evident, like alarm fatigue due to false positives, the complexity in the standardizing detection across different devices, and resource limits that hinder qualitative implementations, thus leaving some vulnerabilities in the healthcare infrastructure. This paper proposes a new Efficient Intrusion Detection model based on the Correlation-Based Feature Selection and the OptCNN-LSTM model to address these problems. The proposed methodology comprises five key phases: (i) Data Acquisition (ii) Pre-processing (iii) Feature Extraction (iv) Feature Selection (v) OptCNN-LSTM Model-based intrusion detection. The raw data is first gathered and then preprocessed using z-score normalization and data cleaning. Then, the best features are extracted using central tendency, the degree of dispersion, and correlation. A mixed IHHO-PSO feature with the Correlation-based Feature Selection (CFS) framework is employed to choose the best features amongst the collected features. At last, the OptCNN-LSTM model is performed to detect the intrusion in the IoMT based on features-selected data. The CNN is tuned using the Levy Flight Optimization (LF) which can be further combined with the LSTM to get the expected results. The code is written in Python and the model is then run to determine its performance which is measured in terms of accuracy, precision, f-measure, and a Receiver Operating Characteristic Curve (ROC). Compared to the current models, the proposed model has the highest accuracies 97.6% and 96.5% for learning rates 70 and 80, respectively…

Keywords: IoMT; Intrusion Detection; Correlation; Feature Selection; ROC

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

1. Introduction

The interconnection of objects and systems through the Internet of Things (IoT) is one of the most dramatic transformations, which is prominent through the enhanced efficiency and the collected important data [1]. The IoT is a network of things that include devices, software and other technologies that are embedded in them so that they can share data as well as communicate with each other. The goal of the IoTM is to integrate IoT into medical programs, monitoring systems, medical equipment and every device related to the healthcare industry [2]. The combination of Informational and Communication Technology and Medical Devices produced IoMT, which is one of the subsets of IoT. The combination of diverse technologies in health care promotes more personalized and effective solutions, which in turn, enables the processes of monitoring, analysis, and management of health-related data. IoT technology is now mainstream and is integrated into medical devices to a point where it can remotely monitor patients and even create intelligent healthcare systems and enable better patient outcomes [3]. Fig. 1 is depicted on the right side of the text as an illustration of IoMT.

While dealing with cybersecurity, intrusion is used for actions or attempts of unauthorized access which might lead to the disruption of a system's security. The process of identifying and implementing proper measures to counteract, unauthorized access, or hacking is called intrusion detection [4]. And it is pertinent to mention that in the context of IoMT intrusion detection should be used to prevent any disclosure or modification of the important medical data [5]. Using intrusion detection in IoMT, patient privacy is protected, early detection of potential breaches and on-the-go threat identification are only a few of the many advantages of this approach. Intrusion detection systems improve the security features of IoMT infrastructures by incessantly monitoring system behaviour and network traffic, which makes sure the accuracy and reliability of medical data [6].

IoMT intrusion detection is very important but the techniques already in use have flaws to it. Quite a number of the current operating systems are based on signature-based detection, which may not be sufficient to detect new or complicated attacks [7]. Moreover, intrusion detection system development is obstructed by resource shortages in IoMT devices including low processing power and energy. In addition to that, standardization of intrusion detection systems becomes more difficult due to the different types of medical devices and communication protocols exploited in IoMT [8].

Healthcare data is vital, which emphasizes the need for intrusion detection in IoMT. Medical data breaches can have serious repercussions, from invasions of privacy to potentially fatal circumstances. IoMT adoption is rising, and with it is the possible threat landscape. Consequently, the integrity and security of healthcare systems depend heavily on efficient intrusion detection systems.

The foremost contributions of this paper are as follows:

- This paper presents a Hybrid IHHO-PSO and Correlation-based Feature Selection Framework and a hybrid deep-learning framework to achieve effective Intrusion detection in an IoMT environment.
- A Hybrid IHHO-PSO feature based on the CFS Framework is introduced to enhance feature selection for efficient intrusion detection in IoMT environments. Combining CFS, Improved Harris Hawks (I-HHO), and Particle Swarm Optimization (PSO), the framework achieves a robust feature selection mechanism, enhancing the entire effectiveness of intrusion detection systems in IoMT.
- An OptCNN-LSTM Model is developed for intrusion detection in the IoMT context which combines OptCNN with LSTM networks. This fusion empowers the model to excel in extracting pertinent features, learning patterns, and adapting to evolving security threats efficiently.

The rest of the section is systematized as Section 2 of this study offers a literature review of the techniques that have been done previously on intrusion detection in IoMT environments, and Section 3 offers the proposed methodology of the suggested model. The result and discussion of the paper are offered in Section 4. Section 5 presents a conclusion of the research study.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

2. Literature review

This section evaluated some of the most recent studies on intrusion detection in IoMT settings.

In 2023, Faruqui et al. [9] addressed the rising cybersecurity threats in the IoMT by suggesting SafetyMed, a novel IDS. SafetyMed used LSTM networks with CNN to achieve a high accuracy of 97.63% in protecting Internet of Medical Things devices from both harmful image data and sequential network traffic. From the study result, it can be said that SafetyMed is a tool that helps to better IoMT security and makes a significant change in some sensitive areas, particularly the medical field.

In 2022, Chaganti and his colleagues [10] examined security problems in IoMT, and they proposed a PSO-DNN (Particle Swarm Optimization Deep Neural Network) for intrusion detection. This method was validated using network traffic and patient sensing datasets, resulting in an impressive 96% accuracy. therefore, they provide DL technology characteristics of safety and reliability that are used by IoMT applications, a paper underlined that they are much better at detecting network intrusion than ML models are.

In 2022, Singh et al. [11] underscored challenges in the COVID-19 pandemic with the overarching theme of the increased use of IoT-enabled medical devices. For IoMT applications it proposed Dew-Cloud-based distribution which can establish data privacy through federated learning in a hierarchical network. The model demonstrated improved performance in comparison with current systems during the test, thus stressing the significance of safeguarding critical medical data on network devices that have limited resources.

In 2023, Norouzi et al. [12] created a secure IoMT environment applying a GA-RF hybrid genetic algorithm-based random forest framework. In medical data safety, the proposed model excelled the AI in malicious attack detection for a high level of precision, accuracy, and recall. According to the experimental outcomes, the GA-RF model comes with the best performance among the machine learning algorithms.

Ravi et al. [13] presented a DL-based method for intrusion detection in the IoMT network in 2023, which achieves a 10-fold cross-validation accuracy of 95% on network features based on the analysis of the network. Application of this framework showed its accuracy on various network-based intrusion datasets and achieved a higher level of performance than previous methods by incorporating a global attention layer and cost-sensitive learning. The suggested model is marketed as an efficient network monitoring tool in the IoMT domain for medical institutions.

In 2023, Alalhareth and Hong [14] brought up the issue of security in IoMT and introduced a deep learning-based (IDS). In this regard, the study emphasizes the analysis of system traffic and biometric data of the patient. The study used the fuzzy logic-based methodology to fine-tune the performance of IDS dynamically and thus increase the precision and effectiveness of intrusion detection in the context of IoMT.

Shambharkar and Sharma et al. [15] in 2023, were the ones to emphasize IoT integration in healthcare paying close attention to IoMT technology. The study simply suggested AI-based techniques that can be used for IoMT network intrusion detection such as ML and DL. There was a secure model proposed to assure patients' data safety in the healthcare IoT environment as the three DL models which performed with a 100 % accuracy rate were presented.

In the year 2020, RM et al. [16] dealt with the problems of IoMT security and specified DNN (deep neural network) as a suitable IDS (intrusion detection system). In terms of accuracy and temporal complexity, the DNN model defeated other machine learning techniques, improving IoMT security and guaranteeing safe data transfer between end users. Reviews of research gaps written by various authors are shown in Table 1.

2.1 Problem Statement

Table 1: Reviews by various authors about the research gaps

Author	Aim	Methodology	Advantages	Drawbacks

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

Name [Citation]				
Faruqui et al. [9]	To address the cyberse curity issues in IoMT utilizing SafetyMed IDS	Novel IDS combining CNN and LSTM	• Using CNN and LSTM simultaneously to improve intrusion detection. • Attained a remarkable 97.63% average accuracy. • Equili • brates the detection rate (DR) and FPR.	• Insufficient details about practical application. • Potential difficulties in interpreting the model.
Chaganti et al. [10]	To investigate the safety and confidentia lity issues associated with IoMT using PSO-DNN	PSO-DNN as an intrusion detection system	• Improved intrusion detection with the proposed Particle Swarm Optimization. • Exhibited an impressive 96% accuracy rate. • Comprehensive assessment of ML and DL techniques.	• Limited investigation of deployment issues in the real world. • A potential susceptibility to modifying hyperparamet ers.
Singh et al. [11]	To propose a Dew-Cloud-based architectur e for IoMT application security	Dew-Cloud model using HFL and HLSTM	• Addresses challenges during the COVID-19 pandemic. • For data privacy, employ hierarc hical federated learning. • Outperformed existing system s in terms of metrics of performance.	• Limited discussion on scalability. • Implementati on issues in the real world are not thoroughly discussed.
Norouzi et al. [12]	To suggest a GA-RF model for an environme nt that is secure for IoMT	Hybrid GA-RF model	• Exhibited superior recall, accuracy, and precision compared to other ML systems. • Uses a hybrid genetic algorithm in conjunction with a random	• Limited examination of the computationa l overhead. • The difficulties of real-world deployment are not sufficiently covered.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

			forest to detect intrusions. • Focus on safeguarding susceptible medical data in IoMT.	
Ravi et al. [13]	To introduce an IoMT intrusion detection technique based on DL	DL model with global attention layer	• Employs DL methods for intrusion detection based on network access. • Achieved a high accuracy 10-fold cross-validation. • To overcome data imbalance, this method employs a cost-sensitive learning mechanism.	• Possible needs for computational resources. • Limited investigation of real-world obstacles.
Alalhareth and Hong et al. [14]	To suggest an IDS for IoMT networks that is DL-based	Deep learning-based IDS	• Offers an approach for intrusion recognition based on deep learning. • Highlights the significance of assessing both network traffic and patient biometric data. • Establishes a fuzzy logic-based approach for efficiency optimization.	• Limited examination of interpretability. • Possible difficulties in real-world implementation.
Shambharkar and Sharma et al. [15]	To demonstrate AI-based intrusion detection and address IoT integration in the healthcare industry	AI-based approaches for intrusion detection	• Highlights the advantages of remote diagnostics and real-time patient monitoring. • Offers three DL models with a 100% accuracy rate. • Addresses the requirement for a reliable and secure approach in	• Limited discussion on practical application difficulties. • In diverse IoT environments, difficulties could arise.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

			IoT for healthcare.	
RM et al. [16]	To suggest an IoMT security DNN-based firewall	DNN model for intrusion detection	• Outperforms current ML techniques in accuracy and time complexity. • Offers a DNN for effective intrusion detection in the IoMT. • We examine in detail the role of pre-processing and classification methodologies.	• Insufficient details regarding scalability. • The practical difficulties of real-world implementation are not sufficiently covered.

3. Proposed Methodology

Implementing an Intrusion Detection Framework in the IoMT serves for around-the-clock monitoring of unauthorized activities, hence the improved real-time security. On the other hand, the utilization of the Hybrid Correlation-based Feature Selection and OptCNN-LSTM Model will contribute to the robustness of the solution because it will be able to capture the spatial and temporal dependencies efficiently. This holistic approach not only reduces the rate of false alarms but also offers a great improvement in cybersecurity in the IoMT networks which provides an answer to the issues of medical device networks. This research presents a framework for Intrusion Detection in the IoMT through a Hybrid Correlation-based Feature Selection and OptCNN-LSTM approach. The methodology encompasses four main stages: Data Acquisition, Pre-processing, Feature Selection, and Intrusion Detection with the Deep OptCNN-LSTM Model. The architecture of the model is presented in Figure 1 as a whole.

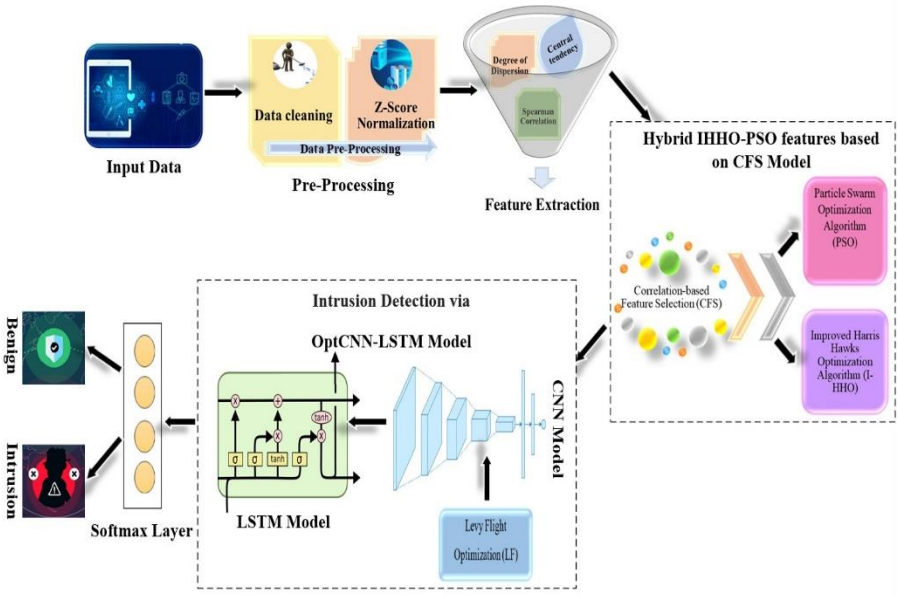


Figure 1: Overall architecture of the suggested model

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

3.1 Data Acquisition

The raw information was taken from WUSTL EHMS 2020 Dataset. This dataset was created utilizing a real-time EHMS testbed. Since there isn't a dataset that incorporates both patient biometrics and network flow metrics, this testbed gathers both data. As illustrated in Fig. 2, the components of the Enhanced Healthcare Monitoring System (EHMS) testbed are healthcare sensors, gateway, system, and control with visual. The gateway receives data from the patient's bodily sensors. After that, the gateway uses the switch and router to deliver the data to the server for visualization. An attacker might intercept these data before they get to the server. The real-time network flow traffic, patient biometric data, and anomaly detection are all handled by the Intrusion Detection System (IDS).

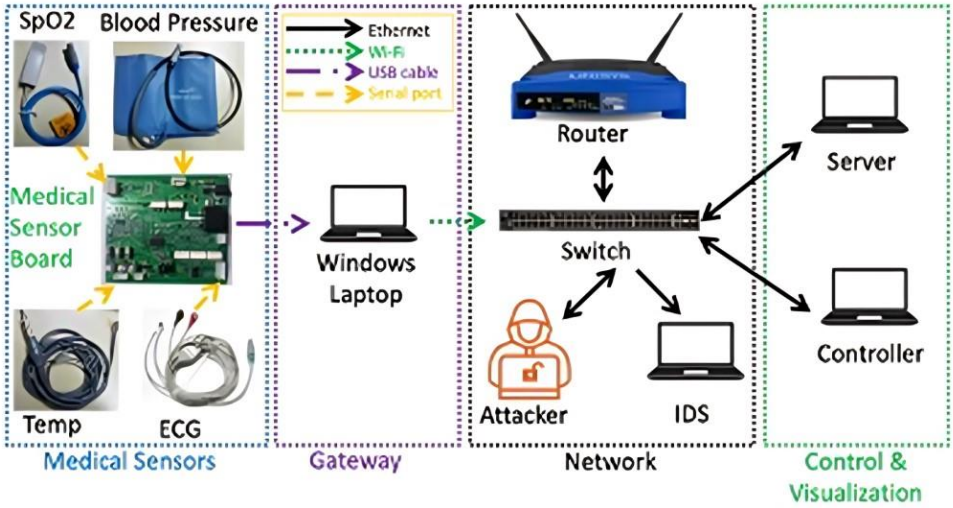


Figure 2: EHMS Testbed

Data shot and spoofing are the two forms of man-in-the-middle attacks present in this dataset. The patient's data confidentially is breached by the spoofing attack, which only detects traffic between the gateway and the server [17]. The integrity of the data is compromised by the data injection attack, which modifies the packets instantly. The Audit Record Generation and Utilization System (ARGUS) tool was employed to record and preserve the network flow traffic as well as the patient's biometric data in a "CSV" file. The statistical data for the WUSTL-EHMS-2020 dataset is displayed in Table 2. There are 44 features in this dataset: one feature for the label, eight biometric features from the patients, and 35 network flow measurements. The invader laptop Medium Access Control (MAC) addresses were labelled as 1 in the samples that contained them, and 0 in the samples that did not have them, according to the Source MAC address functionality used to label the data.

Table 2: Dataset Statistical Information

Measurement	Value
Size of dataset	4.4 MB
The number of attack samples	2,046 (12.5%)
Total quantity of samples	16,318
The number of typical samples	14,272 (87.5%)

The collected raw data are moved on to the next stage.

3.2 Pre-processing

The initial raw data undergoes an intricate pre-processing stage to ensure its quality and suitability for IDS. This step includes Data cleaning and Z-Score Normalization.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

3.2.1 Data cleaning

To guarantee that the correctness of the intrusion detection system by the data cleaning process is feasible. The process of preprocessing and cleaning up of IoMT sensor data comprises several steps. The raw data is collected from different medical tools and sensors, namely wearables and vital sign monitors. Dealing with missing values, outliers, and noise in the first step of the data cleaning process gives the peace of mind that the dataset does not contain peculiarities that could end up sending false alarms or wrong threat detection. Thus the strict data-cleaning procedures allow the IoMT medical data to be more trustworthy and the intrusion detection system to be more effective than the tools before [18].

3.2.2 Z-Score Normalization

Z-score normalization is paramount to IoMT malfunctioning recognition due to abounding data and biodiversity. By applying similar treatment to network traffic, session logs, and user behaviour, enterprises can detect suspicious patterns or anomalies by using statistical methods. The Z-score is expressed by the Eq. below. (1).

$$J = (z - \beta) / \alpha \quad (1)$$

where:

- z: initial amount
- β: data Mean
- α: data Standard deviation

Eq. (1) enables us to figure out the average deviation of any given figure from the mean. the point or z here is where the value of α is the standard deviation and β is the mean. It makes very consistent threshold values possible because all the features that are being handled in the different units and scales will be turned into a common scale through this normalizing process [19]. When it comes to IoMT systems which are all about looking at huge data clusters in real time, Z-score normalization is the tool that makes it easier for the detection of cybersecurity threats by focusing on the deviations that could be covered by different data sizes. By its timely identification of and response to threats to security, it thus ensures the security status of IoMT systems. To obtain the most useful features, the pre-processed data will move to the feature extraction step.

3.3 Feature Extraction

The best features are extracted from the pre-processed data utilizing correlation, degree of dispersion, and central tendency. The central tendency is made up of the geometric mean, median, harmonic mean, mode, and arithmetic mean. Variance, Standard Deviation, Range (max-min), Mean Deviation, and Quartile Deviation are used to process the degree of dispersion. and Spearman correlation is used to process correlation.

3.3.1 Central Tendency

A measure of central tendency is an overall statistic that attempts to characterize a whole collection of data with just one value that stands for the distribution's mean or centre. The central tendency and its mathematical formulations are displayed in Table 3.

Table 3: central tendency and their equations

Features	Formula	Description
Geometric Mean	$\text{Geometric Mean} = D_{IO} = (D_1 \times D_2 \times D_3 \times \ldots \times D_t)^{\frac{1}{\tilde{t}}}$	The $s{-}th$ root of the product of s numbers is the geometric mean. It can be used often to calculate the average growth rate or average ratio.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

Harmonic Mean	$\frac{1}{Q_L} = \frac{1}{r}\sum_{m=1}^{r}\frac{1}{b_m}$ or $Q_l = \frac{r}{\sum_{m=1}^{r}\frac{1}{b_m}}$	The harmonic mean is the reciprocal of the mathematical average of the inverses of a set of numbers. When the average of the rates is required, it is employed.
Arithmetic Mean	$Mean = \frac{\sum_{m=1}^{r} b_m}{r}$	The arithmetic mean of a dataset is calculated by dividing its total value by its entire number of values.

- **Median**

The centre value in a sorted dataset is represented by the median. Unlike mean, median is unaffected by extreme values. For datasets with extreme values, the median is helpful. For the dataset represented in Eq. (2) with odd numbers.

$$median = Middle\ Value \quad (2)$$

For a dataset with an even number, the expression is shown in Eq. (3).

$$median = \frac{Sum\ of\ the\ two\ middle\ values}{2} \quad (3)$$

- **Mode**

The mode, a statistical measure of central tendency, represents the values in a collection that occur most frequently [20]. A dataset's mode is the number or numbers that appear the most frequently in it. Unlike the mean and median, which are always different, a dataset might be unimodal, bimodal, or multimodal.

3.3.2 Degree of Dispersion

The degree of dispersion is a positive real value that represents how homogeneous or heterogeneous the presented data is. If all of the data points in a collection are the same, the Degree of Dispersion will have a value of 0. On the other hand, the measures of dispersion likewise rise in value as the data become more variable. Variance, Standard Deviation, Range (max-min), Mean Deviation, and Quartile Deviation are used to process the degree of dispersion. The Degree of Dispersion and its mathematical expressions are displayed in Table 4.

Table 4: Degree of Dispersion and their equations

Features	Formula	Description
Variance	$\partial^2 = (1/p_1 + p_2) \div \left[p_1\left(\partial_1{}^2 + f_1{}^2\right) + p\left(\partial_2{}^2 + f_2{}^2\right)\right]$ Where, $f_1 = \bar{y}_1 - \bar{y}$, $f_2 = \bar{y}_2 - \bar{y}$, and $\bar{y} = (p_1\bar{y}_1 + p_2\bar{y}_2) \div (p_1 + p_2)$	$\partial_1$and ∂_2 are two standard deviations of two series of sizes $p_1$and p_2 with means $\bar{y}_1$and $\bar{y}_2$.
Standard Deviation	$\delta = \sqrt{\frac{\sum_{l=1}^{q}(L_l - Mean)^2}{Q}}$	Q be the total number of values, L_l is the individual value from 1 to Q.
Range	$Range = A_{max} - A_{min}$	The range, a common dispersion metric, represents the gap between a dataset's

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

		greatest and smallest values.
Mean Deviation	$\sum_{1}^{o} \frac{\lvert Y - \bar{Y} \rvert}{o}$	Where $\bar{Y}$ is the central value and denotes the mean, median or mode.
Quartile Deviation	$\frac{R_3 - R_1}{2}$	Where R_3 *and* R_1 are the third and first quartiles respectively.

3.3.3 Correlation

The Spearman correlation is used to process correlation. To spot potential security risks or unusual activity within a healthcare network, correlation analysis is used to examine the connections between different data points. Correlating data streams including network traffic patterns, device behaviour, and user access logs is essential for spotting anomalies that can point to a cyberattack or unauthorized access in the IoMT, which links medical systems and devices.

- Spearman correlation

A true indicator of the calibre of a monotonic link between matched data is Spearman's connection coefficient. Since Spearman's correlation coefficient measures monotonic relationships, a value does not necessarily indicate that the variables have no link at all. For instance, a perfect quadratic relationship may be seen in the scatter plot below, which suggests a (monotonic) correlation. It is crucial to comprehend Pearson's Correlation, a real indicator of the strength of a straight association between matched data, before understanding Spearman's correlation. The following information presumptions must exist for it to be computed and tested for essentiality.

- interval or ratio level
- linearly related
- Vicariate typically circulated

If the data does not fit the aforementioned assumptions, apply the Spearman's rank connection as shown by Equation (4).

$$s = 1 - \frac{6 \sum g_i^2}{q(q^2-1)} \quad (4)$$

Security systems can detect trends that diverge from typical behaviour by using correlation techniques like Spearman correlation [21]. This allows them to identify and respond to possible attacks instantly, improving the overall cybersecurity posture of IoMT environments. The data proceeded to the feature selection stage following the feature extraction.

3.4 Feature Selection via Hybrid IHHO-PSO based on CFS

From the feature-extracted data, the optimal features are chosen by employing a Hybrid IHHO-PSO based on the CFS approach. The suggested model is a combination of the CFS, I-HHO, and PSO algorithms respectively.

3.4.1 Correlation-Based Feature Selection Approach

The main goal of the filter-based CFS technique is to find the best possible solution in search space by assessing the redundancy and relevance of a chosen feature subset to the class. Features are selected using the correlation function following the outcome of the feature subset assessment. It can be inferred that the selected traits have a maximum degree of relationship with the class, but not with one another. High-scoring features all predict classes in the instance space more accurately than other features, as shown by Eq. 5.

$$E_u = \frac{h\, f e\, h}{\sqrt{h + h(h-1) + fhh}} \quad (5)$$

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

where fhh is the degree of inter-correlation mean between features, $fe\ h$ is the degree of correlation mean between features and the class label, and CS is the assessment for a feature subset of h features. A correlation method based on feature subsets is employed to evaluate CFS. Higher evaluation values therefore result from larger or smaller $fe\ h$ in particular subsets. Lastly, the training and testing sets were reduced utilizing the feature subsets that were chosen and had the highest value, as seen in Fig. 3.

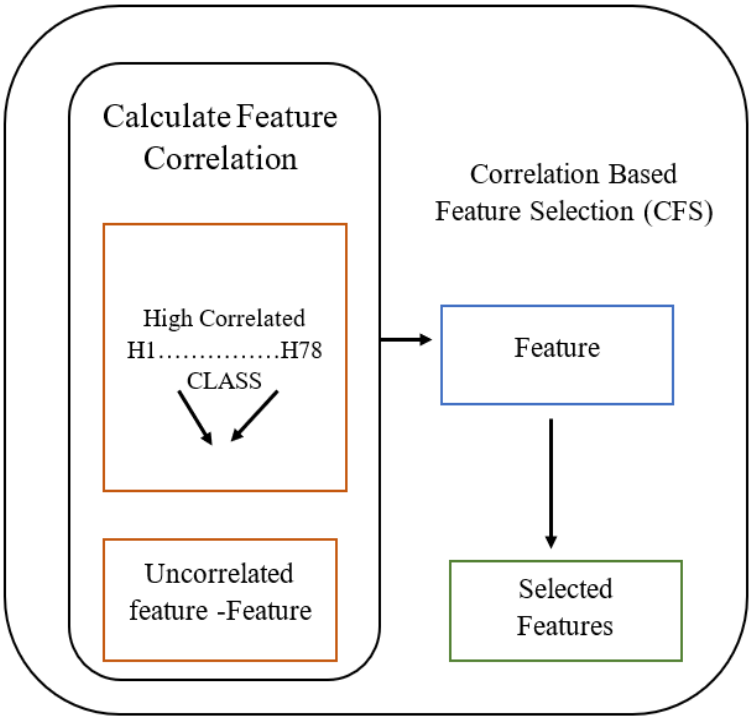


Figure 3: Correlation Based Feature Selection (CFS)

3.4.2 Hybrid IHHO-PSO Model

After performing correlation-based feature selection, the chosen data is then processed using the hybrid IHHO-PSO model to determine the optimal features.

Initialization of I-HHO: The cooperative hunting style exhibited by Harris's Hawks serves as the model for the Harris Hawk Optimization (HHO) algorithm. Using a variety of search operators, it balances exploration and exploitation using a population-based methodology. During optimization, the algorithm constantly modifies its search behaviour to improve performance. Although the HHO algorithm typically yields efficient solutions for optimization problems, premature convergence might pose certain difficulties, especially when tackling intricate issues. This study improved the fundamental HHO algorithm to overcome this constraint and reduce premature convergence. In the first modification, a quasi-oppositional idea is incorporated to enhance the algorithm's speed while addressing its premature convergence tendencies. The quasi-opposite is formulated as presented in Eq. (6) and Eq. (7),

$$Z_{k+1}^{new} = rand\left(\frac{-Z_k+\bar{Z}_k}{2}, a_k\right) \quad (6)$$

$$t_{k+1}^{new} = rand\left(\frac{-t_{m,k}+\bar{t}_{m,k}}{2}, b_k\right) \quad (7)$$

where $-Z_k$ and $\bar{Z}_k$ indicates the lower and the upper limits of the z_k^v and a_k^v outlines the opposite that is definite by the subsequent Eq. (8) and Eq. (9).

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

$$a_k = -Z_k + \bar{Z}_k - Z_k^{new} \quad (8)$$

$$b_k = -t_{m,k} + \bar{t}_{m,k} - t_k^{new} \quad (9)$$

$$k = 1,2, \ldots . F$$

$$m = 1,2, \ldots .5$$

Where F represents the dimensions of the search space. The second improvement involves developing the algorithm's speed, population diversity, and avoidance of the local optimum using chaos theory. To alter the algorithm's performance, the suggested model uses a recognized chaotic mechanism termed a logistic map mechanism. The following Eq. (10) is the formulation of this mechanism:

$$no_{l,p}^{k+1} = 4no_{l,p}^{k}\ (1 - no_{l,p}^{k}) \quad (10)$$

where p is the population number, l is the number of system generators, k denotes the iteration number, and no_p, which is set between 0 and 1, is the quantity of chaotic mechanism at iteration p. The improved version of HHO is shown in Fig. 4. By considering the definitions, the rationalized calculation for the examination is shown in Eq. (11)

$$G = 2 \times no_{iter} \times \left(\frac{V_{iter} - v}{V_{iter}}\right) \quad (11)$$

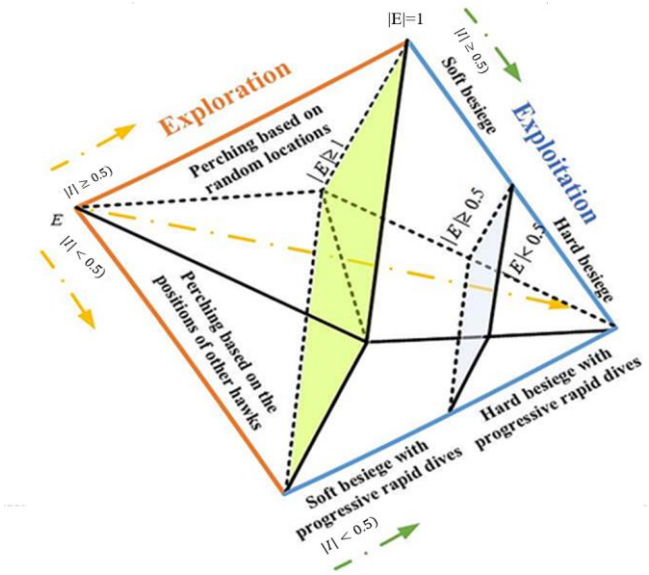


Figure 4: Improved HHO

To select the significant characteristics for intrusion detection, an enhanced Harris Hawk optimization technique is first used, however, it has issues during training. To overcome these constraints and improve the trade-off between the algorithm's examination and corruption capabilities, the I-HHO optimizer and PSO algorithm are combined. The I-HHO algorithm has a limited capacity for exploration because the Hawks must wait anywhere from a few minutes to many hours for prey. By integrating PSO and I-HHO, the algorithm's convergence speed has been increased, removing this constraint. The PSO method is selected due to its exceptional exploration capability and ease of use. The advantages of I-HHO and PSO have been combined to create a Hybrid IHHO-PSO Model, which attempts to achieve a trade-off between exploration and exploitation mechanisms in comparison to I-HHO and other traditional algorithms. Equation (11) is changed during the I-HHO optimization process's exploration phase by integrating the PSO algorithm. The new Eq. (12) and Eq. (13) are as trails:

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

$$A(v+1) = \begin{cases} A_{rand}(v) - u_1 \left| A_{rand}(v) - 2u_2 A(v) + x(v+1) \right. & t \geq 0.5, \\ A_{rab}(v) - A_p(v) - u_3(nq + u_4(wr - nq)) + x(v+1) & t < 0.5, \end{cases} \quad (12)$$

$$x(v+1) = \omega x(v) + e_1 u_1 \{Rn_{dv} - A(v) + e_2 u_2 \{In_{dv} - A(v)\} \quad (13)$$

Algorithm 1 displays the pseudocode for the hybrid I-HHO-PSO algorithm.

Algorithm 1: hybrid I-HHO-PSO Algorithm

Input: Population size, upper and lower boundaries, speeding up coefficient, inertia factor, random factors, and convergence criteria
Output: Where the prey is and how fit it is
The population is set up
While (halting standards)
Do
  Fitness (every Hawk in the population)
if $e\_rfine > rfine$
  Then $rfine = e\_rfine$
else $rfine = rfine$
  $ifine =$ particle possessing the greatest $rfine$ within the populace
Find the rabbit's location
For (Every Hawk)
  Update the prey's starting energy and leaping capability
  Update the prey's energy state
// Exploration phase
$if(|I| \geq 1)$
  Equation (12) modifies each hawk's position within the population.
// Exploitation phase
$if(|I| \geq 1)$
$if(u \geq 0.5 \; and \; |I| \geq 0.5)$
// Soft Besiege
Adapt the Hawks' stance according to the Soft Besiege's expression
// Hard Besiege
else if $(u < 0.5 \; and \; |I| < 0.5)$
Adapt the Hawks' posture
// Soft Besiege with dives
$else \; if \; (u < 0.5 \; and \; |I| \geq 0.5)$
  $C = A_{rab}(v) - I|KA_{rab} - A_o(v)|$
  $D = C + RyLF(I)$
  $A(v+1) = \begin{cases} C & if(H(c) < H(A(v))) \\ D & if(H(D) < H(A(v))) \end{cases}$
else if $(u < 0.5 \; and \; |i| < 0.5)$
  $C = A_{rab}(v) - I|KA_{rab} - A_o(v)|$
  $D = C + RyLF(I)$
  $A(v+1) = \begin{cases} C & if(H(c) < H(A(v))) \\ D & if(H(D) < H(A(v))) \end{cases}$
  return the solution

3.4.3 Hybrid IHHO-PSO features based CFS Selection

To improve the hybrid IHHO-PSO model's feature selection, the CFS classical statistical approach was implemented forth, and Algorithm 1 suggested the hybrid I-HHO-PSO algorithm using the subsequent steps:

1. Use the CFS-based correlation calculation to determine the score for each attribute.
2. Set a threshold and then choose every feature that is greater than it.
3. Apply Hybrid IHHO-PSO to the subset of chosen features.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

4. Additional selection to eliminate redundant features and choose the best group of features.

The feature-selected data moved on to the next stage to detect the intrusion in the IoMT Environment.

3.5 Intrusion Detection Using OptCNN-LSTM Model

From the selected features, the intrusion is detected using the OptCNN-LSTM model, which combines CNN and LSTM. The CNN is optimized through LF and subsequently hybridized with LSTM.

3.5.1 Optimizing CNN using LF

The architecture of the suggested OptCNN-LSTM model is displayed in Fig. 5. The optimized CNN and LSTM sections make up the two elements of the design. It is possible to improve CNN performance by using optimized parameters, such as learning rate, epoch, and weight. CNN's augmented epoch count contributes to improved accuracy. CNN hyperparameters are optimized by the proposed model using the LF method.

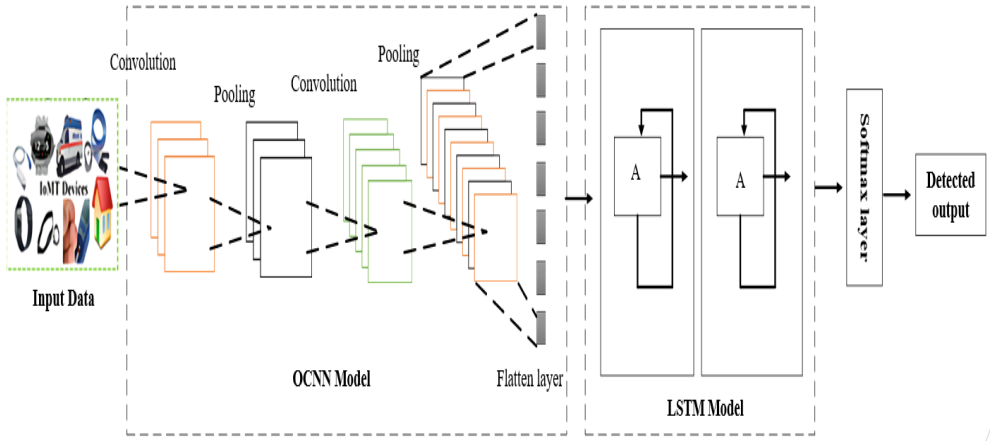


Figure 5: opt CNN-LSTM Model

The CNN architecture contains an input layer, convolutional layer (CL), fully connected layer (FCL), max pooling layer (MPL), and output layer. For the feature extraction task, the CNN's CL layer uses numerous convolutional filters. Consequently, these convolutional filters convolve convolutionally with every input data offset. The CL consists of weights that should be adjusted by employing gradient descent training which changes the parameters of the CL. Here, a nonlinear rectified linear unit (ReLU) activation function is utilized to map the features that have been retrieved from the CL into the feature space. To get the gradients and activations more evenly distributed across the network, a batch normalization layer (BNL) is positioned between the CL and ReLU. The pooling layer (PL) is utilized to hold the most relevant data and decrease the size of the feature maps that are taken from the CL. Max-pooling and average pooling are the two pooling techniques. CNN's PL has no biases or weights for training, unlike other models. The next layer is a fully connected classifier, which classifies the features that are extracted from the MPL and C.

The CNN training process modifies the number of hidden nodes in the fully connected classification layers and the convolutional kernel parameters. SGD training is mostly applied by CNN to tweak the FCL and CL parameters. By updating the network's weights in reverse order, SGD minimizes the cost function. Employing SGD has the drawback of having a lot of hyperparameters that affect how well the network performs.

In this work, LF is used to optimize the hyperparameters of CNN. Hyperparameters are essential for establishing the CNN's accuracy and convergence. Depending on the purpose of the CNN, choosing the network's hyperparameters is crucial. The primary CNN training hyperparameters are learning rate, momentum, number of epochs, and regularization coefficient. The gradient descent algorithm's speed is determined by the learning rate, while the impact of prior weight updates on the present weight update is governed by momentum. The number of epochs determines how many times the learning algorithm adjusts the network parameters depending on the training dataset. Regularization helps the network overcome overfitting. To manage all of these factors, it is thus vital to modify these

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

hyperparameters to assist the network deliver the most accurate outcomes. The LF approach for the optimization of hyperparameters in CNN tuning is presented in approach (2).

Algorithm 2: LF Optimization for CNN hyperparameter tuning

Input: agents B_h, dimension E_o, batch size C_d, input population, and hyper-parameters I1, $I2, I3, and\ I4$. The number of iterations is o. Hfd, the hyperparameter function $I_{ge,}$
Initialization of population Q1, Q2, Q3
Output: Enhanced hyper-parameter
chosen a batch point data example for training
For the number of optimizations o
To search for a desired agent
Locate the optimal suitability function.
Choose the top B1, B2, and B3 search agents.
Update each agent's position by

$$(Pos\_j)^o = \sum_{l=0}^{o} \binom{o}{l} B1^l bBo^{o-l}$$

Where o is the number of repetitions and l location variation
end for
update $Q_{1,}Q_{2,}and\ Q_3$
End
Sigmoid function $(I_{1,}I_{2,}I_{3,}I_{4,}I_{fd})$
End

3.5.2 Hybridizing the OptCNN with LSTM

At first, the CNN model is trained to capture meaningful information, however, its ability to discern interdependencies among features is limited by the absence of temporal data. To train the system more robustly for efficient feature learning, the improved CNN is hybridized with an LSTM model. By using this approach, the gradient ascends and descend issue was resolved, leading to a higher detection accuracy and a decrease in FPRs. The outputs of the LSTM and OptCNN models are combined and sent into the following layer, which performs a binary classification for intrusion prediction using the single output tensor as a single input tensor. Each model consists of multiple layers. OptCNN consists of two convolutional layers that combine 64 and 50 filters, each of size 1. The layer following it is a max-pooling layer of size 1. The flattened layer is the last in the OptCNN model. In addition, two LSTM layers comprising 70 and 50 neurons are included. Each was followed by a 0.1 dropout to lessen the model's overfitting. All model layers use ReLU as the activation function, except the output layer, which uses Softmax. The loss function that is employed is binary cross entropy. The final output is obtained from the softmax layer.

4. Result and discussion

In this subsection, the results and discussion of the suggested framework are presented. This paper introduces an OptCNN-LSTM model, consisting of Optimized CNN and LSTM components. Various metrics like sensitivity, accuracy, specificity, precision, FNR, FPR, NPV, F-Measure MCC, and ROC have been considered to assess the performance effectiveness of the recommended technique. To demonstrate the execution improvement of the newly established model, it is compared with existing models, including DNN, GA-RF, PSO-DNN, CNN-LSTM, CNN-FL, and LSTM-FL.

4.1 Evaluation setup

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

The proposed framework has been implemented in Python. The suggested model has been evaluated utilizing the WUSTL EHMS 2020 Dataset. 30 percent was utilized for testing 70 percent was used for training then 20 percent was used for testing and 80 percent was used for training. Using cutting-edge methods, a comparative analysis has been conducted. The assessment considered various metrics like sensitivity, specificity, accuracy, precision, FPR, FNR, NPV, F-Measure MCC, and Receiver Operating Characteristic Curve (ROC).

4.2 Parameters of Performance Analysis

The suggested model's performance was assessed utilizing the following metrics sensitivity, specificity, precision, accurateness, FPR, NPV, FNR, F-Measure, and MCC.

i) Accuracy

The degree to which measurements of a quantity are closest to that quantity's actual (true) value is measured by accuracy. Eq. (14) is the accuracy formula's mathematical representation.

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (14)$$

ii) Precision

The portion of documents that are relevant to the discovery is known as precision. The mathematical model is displayed in Eq. (15).

$$Precision = \frac{TP}{FP+TP} \quad (15)$$

iii) Sensitivity

The entire positives divided by the proportion of actual positive forecasts yields the sensitivity value. The mathematical model is displayed in Eq. (16).

$$Sensitivity = \frac{TP}{TP+FN} \quad (16)$$

iv) Specificity

The percentage of accurately anticipated negative consequences and overall unfavourable outcomes is a well-defined measure of specificity. The specificity formula is mathematically presented in Eq. (17).

$$Specificity = \frac{TN}{FP+TN} \quad (17)$$

v) F-Measure

The F-Measure number strikes a compromise between fully recognizing every data bit and guaranteeing that each definition only identifies one type of information item. Eq. (18) provides the mathematical formula for the F-Measure.

$$F\_Score = \frac{Presision.Recall}{Presision + Recall} \quad (18)$$

vi) NPV

The NPV is an arithmetical metric that evaluates the validity of a negative test result in a group of individuals with a particular disease. By separating the total number of individuals without the condition by the number of genuine negatives, one can get the Negative Predictive Value (NPV). The success of detection is evaluated using NPV. Eq. (19) provides a mathematical representation of the NPV formula.

$$\mathrm{NPV} = \frac{\mathrm{TN}}{\mathrm{TN+FN}} \quad (19)$$

vii) FPR

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

By dividing the total number of negative events that are inaccurately categorized as positive by the total number of negative occurrences, the False Positive Rate (FPR) is determined. The FPR formula's mathematical formulation is given by Equation (20).

$$FPR = \frac{FP}{FP+TN} \quad (20)$$

viii) FNR

It is possible for a test to miss detecting a true positive, which is familiar as the false-negative rate or "miss rate." Eq. (21) offers the mathematical representation of the FNR formula.

$$FNR = \frac{FN}{FN+TP} \quad (21)$$

ix) MCC

Due to its consideration of TP, TN, FN, and FP, MCC is a reliable statistic for assessing the performance of binary classifiers. MCC measures how closely the predictor and the actual labels are correlated. Eq. (22) provides a mathematical representation of the MCC formula.

$$MCC = \frac{(TP*TN)-(FP*FN)}{\sqrt{(TP+FP)(TP+FN)(FP+TN)(TN+FN)}} \quad (22)$$

4.3 Overall performance analysis: Learning Rate 70

This section presents an overall performance study for learning rates of 70, taking into account methods based on classifiers as well as those based on algorithms.

4.3.1 Performance Analysis of Learning Rate 70: Classifier

In this section, the performance evaluation of various intrusion detection models is presented. Table 5 displays a comparative analysis of the presented framework and existing models based on performance metrics.

Table 5: Comparative analysis of performance metrics with existing models

Classification Models	LSTM-FL	CNN-FL	CNN-LSTM [9]	PSO-DNN [10]	GA-RF [12]	DNN [16]	Proposed
Accuracy	0.857747	0.797765	0.897476	0.902766	0.934343	0.945636	0.976545
FPR	0.034545	0.047748	0.036466	0.010989	0.034455	0.026374	0.009899
Specificity	0.743457	0.709001	0.823114	0.812003	0.876666	0.897748	0.953561
Precision	0.794656	0.736665	0.845663	0.835434	0.897473	0.909886	0.937765
Sensitivity	0.886646	0.835465	0.915535	0.923098	0.927748	0.957738	0.989977
NPV	0.808348	0.756365	0.835546	0.809965	0.846637	0.847378	0.939878
FNR	0.036636	0.047758	0.034523	0.028758	0.024445	0.02099	0.006578
MCC	0.845664	0.777467	0.856637	0.838766	0.908878	0.864578	0.954877
F-Measure	0.760915	0.720341	0.809811	0.809145	0.894758	0.854648	0.942231

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

Comparing the proposed OptCNN-LSTM model against current intrusion detection methods for the IoMT, significant improvements can be detected in several performance parameters. It is noteworthy that it outperforms LSTM-FL, CNN-FL, CNN-LSTM, PSO-DNN, GA-RF, and DNN, with a maximum accuracy of 97.65%. OptCNN-LSTM outperforms all other models in terms of sensitivity, precision, and specificity, with values of 93.77%, 98.99%, and 95.36%, respectively. The evolution model proposed also attains a maximum F-Measure, which is the measure that is in between sensitivity and precision and shows a solid overall performance. The OptCNN-LSTM model has additionally demonstrated its robustness, with the Matthews Correlation Coefficient (MCC) reaching the highest value of all models, which is 95.49%. In addition, the model gives the lowest FPR (0.66%) and FNR (0.99%), which underscores its capability to reduce both types of errors. The excellent negative predictive value of 93.99% demonstrated that the designed model is very accurate in recognizing non-intrusive ones. The comparative research displays that in contrast to other models, the OptCNN-LSTM model is way much better and more accurate for intrusion detection in the IoMT context.

4.3.2 Performance Analysis of Learning Rate 70: Algorithmic

Here, the evaluations of various algorithms are performed according to their performances. Table 6 in the context of the same learning rate of 70 has a comparison of algorithmic models.

Table 6: Comparative Analysis of Algorithmic Learning Rate 70

Algorithmic Models	WDO	EVO	FOA	ZOA	Proposed
Precision	0.709876	0.786766	0.886766	0.734677	0.937765
F-Measure	0.732354	0.840986	0.825754	0.734677	0.953547
Sensitivity	0.807763	0.897765	0.948762	0.846663	0.989977
Specificity	0.745664	0.823477	0.874554	0.722456	0.944345
NPV	0.743578	0.879877	0.843566	0.768988	0.939878
Accuracy	0.766748	0.867664	0.934568	0.798767	0.976545
MCC	0.724555	0.809868	0.859878	0.786543	0.954877
FNR	0.037877	0.03981	0.015644	0.02491	0.006578
FPR	0.036432	0.024246	0.029801	0.037544	0.00999

The study that compares the proposed models' ability versus optimum algorithms including WDO, EVO, FOA, and ZOA shows that the proposed model is better in various metrics. The proposed model beats WDO with 97.65% accuracy, whereas it is higher than EVO (86.77%), FOA (93.46%), and ZOA (79.88%) with an accuracy of 97.65%. Additionally, the proposed model is demonstrated to have considerably high precision, sensitivity, and specificity with the respective values of 93.78%, 98.99%, and 94.43%. The model in question is an overall good performer as demonstrated by a large F-Measure, which strives to maximize the balance between precision and sensitivity. The solidity of the suggested approach is augmented with the help of Matthew's Correlation Coefficient (MCC) getting a value of 95.49% which is far greater than the existing optimization methods. Besides, this model has a minimum False Negative Rate (FNR), which is equal to 0.66% and a low False Positive Rate (FPR), of 0.99%, meaning that it can be guaranteed to reduce both the false positive and false negative kinds of error. The model proposed above has a 93.99% Negative Predictive Value (NPV) that signifies its capability of correctly detecting non-concerning situations. In general, the comparative analysis outcomes show

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

that the suggested model demonstrated superior performance as compared to other optimization algorithms in terms of intrusion detection metrics.

4.4 Overall performance analysis: Learning Rate 80

This part presents the overall performance analysis of learning rates of 80 which is managed by both classifier-based and algorithmic-based approaches.

4.4.1 Performance Analysis of Learning Rate 80: Classifier

In this part performance evaluation of different algorithmic models will be presented. Table 7 below shows the comparative analysis of classifier models with a learning rate of 80.

Table 7: Classifier-based Performance Analysis of Learning Rate 80

Classification Models	LSTM-FL	CNN-FL	CNN-LSTM [9]	PSO-DNN [10]	GA-RF [12]	DNN [16]	Proposed
MCC	0.815356	0.756637	0.876636	0.898777	0.836646	0.907748	0.952021
Precision	0.803553	0.74202	0.834665	0.876578	0.876476	0.897748	0.943551
Sensitivity	0.896647	0.824553	0.933775	0.943457	0.918247	0.937475	0.976654
Accuracy	0.864775	0.787746	0.925553	0.936647	0.908838	0.927476	0.965099
F-Measure	0.820911	0.733173	0.810923	0.81246	0.898884	0.876748	0.939095
FNR	0.057736	0.059988	0.030994	0.0268	0.027478	0.019988	0.012123
FPR	0.066647	0.046626	0.038778	0.027767	0.035564	0.012375	0.010099
NPV	0.788387	0.746255	0.856212	0.885666	0.876364	0.84897	0.923456
Specificity	0.833422	0.712331	0.804501	0.835109	0.877456	0.834759	0.954233

Considerable distinction within different models is brought out by the classifier-based performance study for learning rate 80, where the suggested model has a strong performance in intrusion detection. The suggested model's accuracy is remarkable at 96.51%; it outperforms CNN-FL (78.77%), LSTM-FL (86.48%), CNN-LSTM (92.56%), PSO-DNN (93.66%), GA-RF (90.88%), and DNN (92.75%). The model's advantage is also illustrated by the values of 94.36% for precision, 97.67% for sensitivity and 95.42% for specificity. The introduced model is more robust than other models, as evidenced by its higher F-Measure, MCC, and NPV values. The proposed model's low FPR and FNR indicate the accuracy, which means that the model does well for these two kinds of errors. In light of the discussed data, the comparison shows that the suggested classifier has a high accuracy of intrusion recognition, but it can learn at the rate of 80. This makes the model an excellent candidate for the implementation of intrusion detection systems.

4.4.2 Performance Analysis of Learning Rate 80: Optimizer

In the next part, the assessment of different algorithm models is described in detail. Table 8 illustrates the different models of algorithmic models with a learning rate of 80.

Table 8: Optimizer-based Performance Analysis of Learning Rate 80

Algorithmic Models	WDO	EVO	FOA	ZOA	Proposed

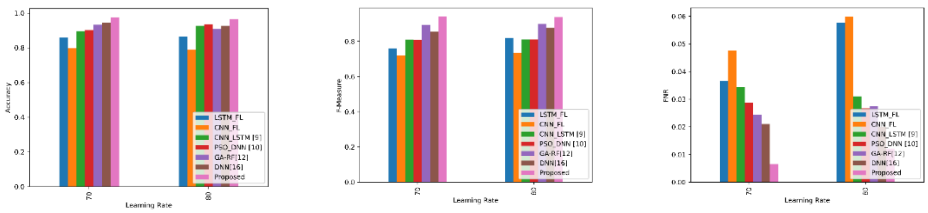
Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

Precision	0.809977	0.743433	0.867758	0.798767	0.943551
NPV	0.813567	0.756775	0.823645	0.721234	0.923456
Sensitivity	0.921233	0.826645	0.946576	0.865544	0.976654
Specificity	0.842343	0.754345	0.823435	0.809221	0.930123
FPR	0.030123	0.047737	0.035512	0.03578	0.00754
Accuracy	0.875666	0.789888	0.935547	0.834434	0.965099
FNR	0.038009	0.038578	0.023455	0.020912	0.006512
F-Measure	0.834567	0.772357	0.841002	0.712346	0.953401
MCC	0.843344	0.797466	0.874665	0.754332	0.932021

The presented intrusion detection model shows its superiority to well-known optimization algorithms, like WDO, EVO, FOA, and ZOA, in the comparative optimizer-based study at a learning rate of 80. The suggested model is ahead of the other models with an accuracy of 96.51%, which proves the model has a remarkable ability to classify the cases of intrusion and non-intrusion. Precision, the accuracy of a positive prediction, hits its peak of 94.36% showing a low false positive rate. Sensitivity, or recall, is 97.67%, indicating how well the model identifies the cases of the intrusion. Moreover, it gets the highest specificity of 95.01%, which shows that it has high a capacity to correctly detect negative cases and a few false negatives. The proposed approach values the whole efficiency by giving the balancing act between sensitivity and particularity at the F-Measure. One of the features which is emphasized by the R-squared model is the model's ability to take into account true and false positives as well as negatives. It can be seen from Matthew's Correlation Coefficient (MCC) which reaches the value of 93.20%. The model with the 92.35% NPV (Negative Predictive Value) is very precise in predicting non-invasive events. However, other factors than the model's recognition of the two kinds of errors contribute to its effectiveness in error reduction. For instance, the model has a low FPR and FNR: 0.65% and 0.75%, respectively. Altogether the suggested model demonstrates to be a holistic and balanced solution for intrusion detection revealing superior performance in all aspects of the evaluation metrics by the learning rate of 80.

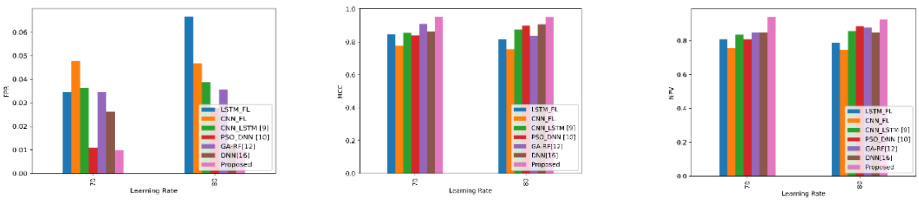
4.5 Graphical representation

In this section, you will see classifier models and algorithmic models with learning rates of 70 and 80 drawn graphically. Fig.6(a)-(e) demonstrates the graph of classifier models with learning rates of 70 and 80.

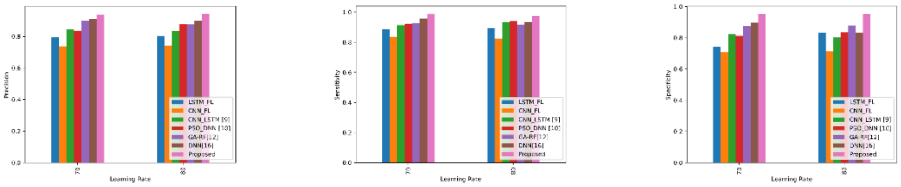


(a) Accuracy (b) F-Measure (c) FNR

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024



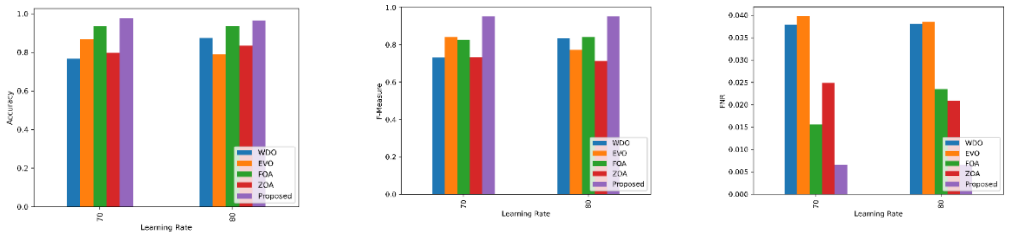
(d) FPR (e) MCC (f) NPV



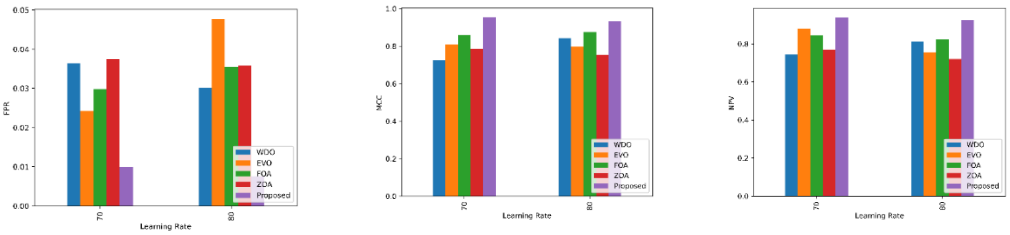
(g) Precision (h) Sensitivity (i) Specificity

Figure 6 (a)-(e): Graphical representation of the classifier models with learning rates of 70 and 80

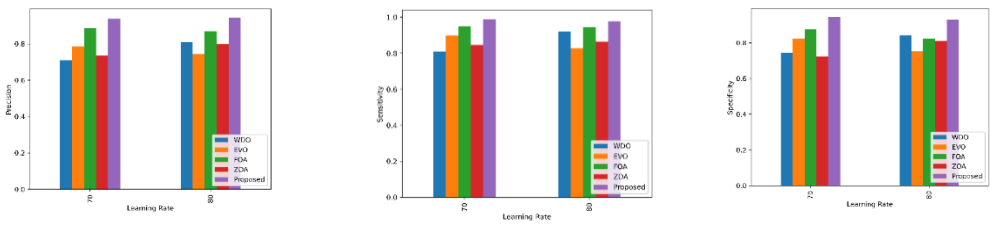
Fig.7 (a)-(e) shows the graphical representation of the Algorithmic models with learning rates of 70 and 80.



(a) Accuracy (b) F-Measure (c) FNR



(d) FPR (e) MCC (f) NPV



(g) Precision (h) Sensitivity (i) Specificity

Figure 7 (a)-(e): Graphical representation of the Algorithmic models with learning rates of 70 and 80

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

Receiver Operating Characteristic Curve (AUC-ROC): Deep learning methods use the AUC-ROC to calculate a binary classification model's efficacy. By generating the ROC curve, it assesses the model's capacity to discriminate between the two classes, which are generally a positive class and a negative class. Plotting the TPR (Sensitivity) against the FPR (1 - Specificity) at different thresholds that the model employs to classify data points results in the ROC curve. The ROC curve shows the trade-off between correctly classifying positive cases (True Positives) and erroneously classifying negative cases (False Positives) when the threshold varies. There is a unique threshold associated with each point on the curve. The AUC-ROC is a single scalar value that represents the entire ROC curve. It lies in the range of 0 to 1, where:

- ✓ AUC-ROC ≈ 0.5: There is little difference between the model and chance guesses.
- ✓ AUC-ROC in the range of 0.7 to 0.8: The model's discriminating power is moderate.
- ✓ AUC-ROC between 0.8 and 0.9: This indicates that the model can discriminate well.
- ✓ AUC-ROC > 0.9: The model's capacity for discriminating is outstanding.

The capability of a binary classification model to differentiate between classes is assessed by the AUC-ROC, which is, in essence, a helpful statistic. It also provides a reliable way to measure the overall performance of the framework over a variety of categorization thresholds. The proposed model's ROC curve value of 0.98 indicates how well it can discriminate. The illustration of the receiver operating characteristics is shown in Fig 7.

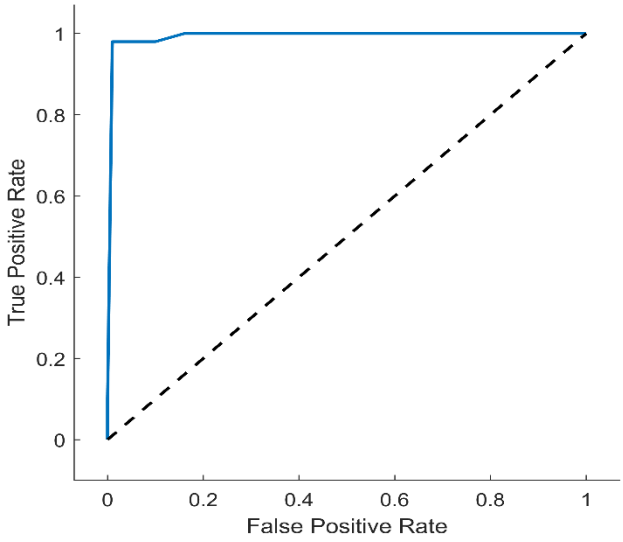


Figure 7: Receiver Operating Characteristic Curve

5. Conclusion

The paper discussed an effective intrusion detection method in an IoMT environment featuring a Hybrid Correlation-based Feature Selection and the OptCNN-LSTM Model. The methodology encompassed several stages, with raw data collection from the WUSTL EHMS 2020 Dataset being the first one among them. After that, the data was given to pre-processing which has Z-Score Normalization and data cleaning. Following pre-processing, correlation, degree of dispersion, and central tendency analysis were employed to extract the best characteristics from the data. Then, to choose the most essential features, a Hybrid IHHO-PSO based on the CFS Framework was used. This hybrid model combines the PSO Algorithm, Improved HHO, and Correlation-based Feature Selection (CFS). DL algorithms have the potential to extract appropriate attributes for automatic categorization, in place of the necessary extraction phase required by traditional machine learning (ML) techniques. This may result in the creation of an all-encompassing security architecture. As a consequence, when LSTM was optimized via LF, it was hybridized with CNN to generate OptCNN-LSTM, a highly scalable malware detection system for the IoMT. The results came from the softmax layer. The Python platform was used to analyze the performance of the suggested model, looking at metrics including accuracy, precision, NPV, F-Measure, FNR, FPR, MCC, and the ROC curve. The suggested model performed very well at learning rates 70 and 80, with astounding accuracy rates of 97.6% and 96.5%,

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

respectively. It also exhibited impressive precision rates of 93% and 94%, outperforming previous models in this field. Additionally, the model showcased strong F1 Scores of 94.2% and 93.9% and achieved high sensitivities of 98.9% and 97.6%. Notably, it attained specificities of 95.3% and 95.4% and MCC values of 95.4% and 95.2% for the two learning rates, respectively. Moreover, the proposed model distinguished itself on the ROC curve with a notable area under the curve (AUC) value of 0.98, improving its class discrimination capability.

References

[1] Gokhale, P., Bhat, O. and Bhat, S., 2018. Introduction to IOT. International Advanced Research Journal in Science, Engineering and Technology, 5(1), pp.41-44.

[2] Villegas-Ch, W.; García-Ortiz, J.; Urbina-Camacho, I. Framework for a Secure and Sustainable Internet of Medical Things, Requirements, Design Challenges, and Future Trends. Appl. Sci. 2023, 13, 6634. https://doi.org/10.3390/app13116634

[3] Das, P.K., Zhu, F., Chen, S., Luo, C., Ranjan, P. and Xiong, G., 2019, June. Smart medical healthcare of Internet of Medical Things (IOMT): Application of non-contact sensing. In 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 375-380). IEEE.

[4] Javaid, A., Niyaz, Q., Sun, W. and Alam, M., 2016, May. A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (pp. 21-26).

[5] Hady, A.A., Ghubaish, A., Salman, T., Unal, D. and Jain, R., 2020. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access, 8, pp.106576-106584.

[6] Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J.C. and Rodriguez, J., 2021. An anomaly-based intrusion detection system for Internet of Medical Things networks. Electronics, 10(21), p.2562.

[7] Binbusayyis, A., Alaskar, H., Vaiyapuri, T. and Dinesh, M., 2022. An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. The Journal of Supercomputing, 78(15), pp.17403-17422.

[8] Mishra, P.; Singh, G. Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects. Appl. Sci. 2023, 13, 8869. https://doi.org/10.3390/ app13158869

[9] Faruqui, N., Yousuf, M.A., Whaiduzzaman, M., Azad, A.K.M., Alyami, S.A., Liò, P., Kabir, M.A. and Moni, M.A., 2023. SafetyMed: a novel IoMT intrusion detection system using CNN-LSTM hybridization. Electronics, 12(17), p.3541.

[10] Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A. and Bhushan, B., 2022. A particle swarm optimization and deep learning approach for intrusion detection system in the internet of medical things. Sustainability, 14(19), p.12828.

[11] Singh, P., Gaba, G.S., Kaur, A., Hedabou, M. and Gurtov, A., 2022. Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE Journal of Biomedical and Health Informatics, 27(2), pp.722-731.

[12] Norouzi, M., Gürkaş-Aydın, Z., Turna, Ö.C., Yağci, M.Y., Aydin, M.A. and Souri, A., 2023. A Hybrid Genetic Algorithm-Based Random Forest Model for Intrusion Detection Approach in Internet of Medical Things. Applied Sciences, 13(20), p.11145.

[13] Ravi, V., Pham, T.D. and Alazab, M., 2023. Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. IEEE Internet of Things Magazine, 6(2), pp.50-54.

[14] Alalhareth, M. and Hong, S.C., 2023. An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning. Sensors, 23(22), p.9247.

[15] Shambharkar, P.G. and Sharma, N., 2023. Artificial Intelligence-driven Intrusion Detection Framework for the Internet of Medical Things.

[16] RM, S.P., Maddikunta, P.K.R., Parimala, M., Koppu, S., Gadekallu, T.R., Chowdhary, C.L. and Alazab, M., 2020. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communications, 160, pp.139-149.

[17] Hady, A.A., Ghubaish, A., Salman, T., Unal, D. and Jain, R., 2020. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access, 8, pp.106576-106584.

[18] Taouali, O., Bacha, S., Ben Abdellafou, K., Aljuhani, A., Zidi, K., Alanazi, R. and Harkat, M.F., 2023. Intelligent Intrusion Detection System for the Internet of Medical Things Based on Data-Driven Techniques. Computer Systems Science & Engineering, 47(2).

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024

[19] Panda, S.K. and Jana, P.K., 2018. Normalization-based task scheduling algorithms for a heterogeneous multi-cloud environment. Information Systems Frontiers, 20, pp.373-399.
[20] Perumal, R. and Venkatachalam, S.B., 2023. Non-Invasive Decay Analysis of Monument Using Deep Learning Techniques. Traitement du Signal, 40(2).
[21] Sharma, A. and Suryawanshi, A., 2016. A novel method for detecting spam email using KNN classification with spearman correlation as distance measure. International Journal of Computer Applications, 136(6), pp.28-35.

Doi: https://doi.org/10.54216/FPA.160112
Received: July 11, 2023 Revised: November 09, 2023 Accepted: April 26, 2024