INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

An Internet of Medical Things and Deep Learning-Based Intelligent Security Framework for Heart Health

V. Maruthi Prasad[1]*, **B. Bharathi**[2]

1 Research Scholar, Department of CSE, Sathyabama Institute of Science and Technology, Deemed to be University, Jeppiaar Nagar, Chennai, Tamil Nadu- 600119, India
2 Research Supervisor, Department of CSE, Sathyabama Institute of Science and Technology, Deemed to be University, Jeppiaar Nagar, Chennai, Tamil Nadu 600119, India

OPEN ACCESS

Received: 22/10/2024

Accepted: 25/01/2025

Published: 12/07/2025

Citation: Maruthi Prasad V, Bharathi B (2025) An Internet of Medical Things and Deep Learning-Based Intelligent Security Framework for Heart Health. Indian Journal of Science and Technology 18(26): 2100-2110. https://doi.org/10.17485/IJST/v18i26.3485

* **Corresponding author**.

maruthi.vv@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: This study aims to address the growing network security risks posed by the increasing integration of IoMT infrastructure into medical facilities. The main goal is to develop and propose the Duo-Secure IoMT architecture that effectively counters complex cybersecurity threats such as botnet-driven distributed denial of service (DDoS) attacks and zero-day attacks while maintaining the integrity of clinical data. **Methods:** The Duo-Secure IoMT framework uses multimodal sensory cues to differentiate between typical IoMT data behaviour and patterns of malicious attacks. To analyze sensory data gathered by IoMT devices, it combines a stacked Bidirectional-LSTM model with a dynamic fuzzy clustering algorithm. By constantly monitoring and analyzing IoMT traffic, this two-stage methodology is intended to identify complex attack patterns within the network. The framework's capacity to anticipate cardiac abnormalities and identify network malware in a distributed IoMT network environment is illustrated using a case study of heart disease that includes 18,940 data points and 36 factors. **Findings:** The Duo-Secure IoMT framework demonstrates an impressive 92% accuracy rate in predicting cardiac anomalies, highlighting its effectiveness in medical diagnosis in the IoMT context. Additionally, it achieves 98.50% accuracy in detecting network malware, making it a reliable tool for identifying potential security threats in IoMT infrastructure. **Novelty:** This study makes a novel contribution by combining multimodal sensory data with sophisticated machine learning methods, specifically by combining stacked Bidirectional-LSTM models with dynamic fuzzy clustering. Traditional security techniques might overlook intricate attack patterns, but this method enables the Duo-Secure IoMT framework to recognize them. Additionally, by attaining high accuracy in malware detection and medical anomaly prediction, the framework offers a revolutionary way to increase cybersecurity resilience in IoMT-based healthcare facilities.

Keywords: IoMT Security; Multi-modal Anomaly Detection; Bi-LSTM Architecture; Network Flow Analysis; Data Balancing Techniques; Feature Selection Methods

1 Introduction

The advent of IoT, particularly in the IoMT domain, emphasizes the integration of smart medical devices. However, this interconnectedness brings forth security concerns, making medical technology susceptible to cyber-attacks. Proactive measures are crucial to pre-emptively address vulnerabilities and potential risks in IoMT infrastructure. IoMT plays a pivotal role in real-time management and remote monitoring across various industries. Effective data management is highlighted as a critical factor, distinguishing IoT from traditional data processing methods. The versatility and distinctiveness of IoT lie in its ability to dynamically process data generated by machines in real-time.

The paper explores the unauthorized access and alteration of user data through malicious network activities. Two types of IDS are examined to systematically monitor and detect such intrusions, addressing the challenges of recognizing novel attacks and deviating transactions. Hackers exploit vulnerabilities in open servers, emphasizing the importance of addressing application flaws, system configurations, and network security issues in IoMT servers. The significance of monitoring data flow and resolving application issues is discussed in the context of thwarting infiltration attempts. A secure, transparent, and patient-driven network for managing medical records is being advanced by blockchain technology in the realm of electronic health records. Data generated by smart Internet of Things devices cannot be stored in RPM (Remote Patient Management) environments using this new technology

Attacks against IoMT can be passive or active, internal or external. Because of weak authentication protocols and subpar design, a hacker could stop sensitive and crucial data from being sent between medical devices and Fog before it even gets to the Internet. This gives a hacker the ability to execute various cyber-attacks, including ransomware, spoofing, jamming, and B DoS attacks. Any threat to these devices' security can also result in serious issues like slower interactions or inaccurate diagnoses. A breach of patient privacy can result in serious health issues and even fatalities. This means that in order for IoMT adoption to be successful and continue to grow rapidly in the future, security must be carefully considered from the start.

1.1 Motivations and contribution

The security of IoMT systems is at risk due to vulnerabilities, prompting the need for proactive measures to safeguard operations and medical data integrity. To tackle network security challenges, the document introduces IDS and ML algorithms as tools. With more medical devices connected to the internet, there's a bigger risk of hackers breaking in. Current systems might not catch new types of attacks, leaving devices vulnerable. Some systems might make mistakes and either raise false alarms or miss real threats. The Mirai botnet is exemplified in discussing three deep learning algorithms, including a heuristic-based IDS and ML approaches. A novel solution, the IoMT Duo-Secure framework, is presented, employing multi-modal techniques to address network security issues. By integrating dynamic fuzzy clustering and customized Bidirectional-LSTM algorithms, the framework aims to concurrently detect anomalous patterns and perform data assessments.

This study underscores the primary contributions in the development of the Duo-Secure IoMT framework. The proposed solution addresses uncertainty surrounding anomalous network attacks, ensuring the seamless operation of IoMT systems by effectively identifying and mitigating anomalous network activities. Following a structured approach, the article provides an overview of relevant research, delves into materials and techniques employed, presents findings and analysis, and concludes with final remarks. The comprehensive list of references consolidates the study within the existing body of knowledge.

1.2 Related Works

Deep learning techniques and Internet of Medical Things (IoMT) technologies in healthcare have been the focus of several published articles. This section gives a quick summary of the research and discusses IoMT technologies used in CVD as well as systematic reviews of deep learning methods and their outcomes. We discovered that some of these articles concentrated solely on deep learning methods and how they affected a particular disease, while others addressed disease surveillance technologies.

The Ensemble Deep Learning System for Health (EDL-SHS) was developed [(1)] to automate the heart disease detection process in a cloud computing environment with integrated Internet-controlled devices. Using Internet of Things devices, the concept of "Health Fog" in this instance provides medical treatment as a "fog" that efficiently manages patients' cardiac data in response to user requests. When assessing the model's effectiveness, the fog-busting core looks at things like latency, black band, energy consumption, errors, precision, and execution time. For a variety of fog computing scenarios, Health-Fog's adaptability enables customization to customer needs and offers the highest quality of service or prediction accuracy. In order to bridge the resource gap for the high-precision requirements of deep learning, complex deep learning networks can be readily integrated into edge computing paradigms using special communication mechanisms and models like assemblers. Delays are reduced and accuracy is increased as a result.

Sequential forward selection (SFS) feature selection and random forest classification are also combined in an Internet of Things (IoT)-driven hybrid cardiovascular disease prediction system. When compared to other heuristic recommendation systems, this all-inclusive method not only produces accurate predictions but also offers age- and gender-specific body and nutrition advice with an astounding accuracy rate of 98%[(2)]. The Kernel Random Forest data-driven ensemble classifier[(3)] demonstrated its remarkable performance on a dataset of heart disease, achieving an impressive 98% accuracy rate. A new Internet of Things framework that uses wearable sensors and deep convolutional neural networks outperforms logistic regression and other neural networks in terms of accuracy, achieving 98.2% in the collection of blood pressure and ECG data[(4)].

Huang as well as others.[(5)] focused on IoT technologies for health management systems, such as medication management, clinical data management, remote medicine, mobile medical care, clinical device management, and individual health management, in order to provide a basis for future IoT/IoMT security management and design. Lin and associates.[(6)] talked about the most recent developments in the use of flexible sensors for the monitoring of various physiological signals for CVD using pulse wave technology (ECG, PCG, PPG, and SCG/BCG); in particular, they focused on five signal types that can be used to detect CVD using flexible sensing technology. Rahaman and his associates. discussed the advantages and disadvantages of IoT-based smart health monitoring systems and emphasized how these monitoring devices are made and used in relation to patients. They collected 13 studies between 2015 and 2019, accounting for the year, feedback device, key hardware components, price, and usage. Panicker in addition to P. Gayathri [21] separated their work into several categories, including IoT/wearable technology, fuzzy systems, heart sounds, heart images, heart rate variability, feature selection, and predictive models. The different machine learning techniques and data sets that were used, along with the results and any research gaps, were highlighted in the tabulated summary they provided in their review of the literature.

2 Methodology

This section encompasses various aspects, including defining the dataset, outlining pre-processing techniques, detailing data division and normalization procedures, and elucidating the feature selection methodology. The comprehensive mechanism of our contribution is visually presented in Figure 1.

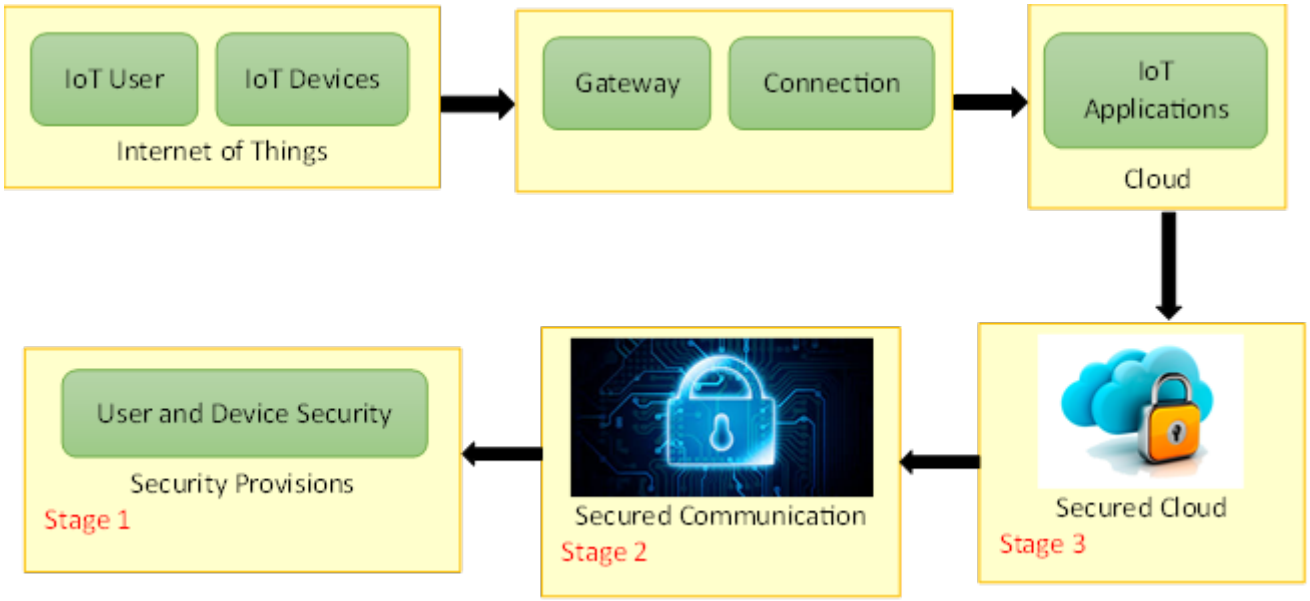

Fig 1. The Comprehensive Mechanism of the Proposed Work

The suggested framework outlines a methodical strategy for enhancing security and boosting effectiveness in IoT systems, with a focus on healthcare monitoring scenarios. The process starts with the careful gathering and pre-processing of the WUSTL-EHMS-2020 datasets, which is based on real-time traffic from the Enhanced Healthcare Monitoring System and includes patient biometrics and network-flow measurements. A strong model architecture is created by skilfully applying cutting-edge deep learning techniques, utilizing bidirectional LSTM networks to effectively capture the temporal trends and

correlations present in the data. The architecture of this model guarantees a thorough understanding of system behaviour, opening the door for improved security features and more efficient operations in IoT ecosystems.

The framework further hones its efficacy through meticulous dataset partitioning, normalization, and judicious feature selection, effectively tackling challenges such as class imbalance and high-dimensional data. By integrating innovative methodologies like fuzzy clustering for feature extraction, the framework augments interpretability and operational efficiency. Rigorous evaluation metrics are meticulously employed to furnish a malicious understanding of the model's capabilities, thereby fortifying its efficacy across diverse real-world scenarios. This holistic approach not only advances the frontier of IoT security but also catalyses advancements in healthcare monitoring systems, nurturing trust and confidence in the robustness of IoT applications, particularly within critical sectors such as healthcare.

2.1 Dataset

In our proposed framework, a comprehensive dataset comprising 16,318 samples was collected, wherein 87.5% of the samples represent normal network behaviour, while the remaining 12.5% correspond to attack instances. The labels 0 and 1 are assigned to non-attack and assault traffic, respectively.

The WUSTL-EHMS-2020 datasets comes from a real-time testbed for the Enhanced Healthcare Monitoring System (EHMS). This dataset contains 44 features in total, including network-flow measurements and patient biometrics. These features include a single label feature, eight patient biometrics, and 35 network-flow measurements. Hady's publication from 2020 provides an explanation of the dataset's origin and structure.

Initially accessible in packet capture (pcap) format, we segmented the data using the SplitCap software. An open-source network traffic flow analyzer called CIC Flow Meter was then used to create Bi-flows from the pcap files and extract pertinent features from them. Algorithm 1 describes the complete data pre-processing procedure for flow measurements and biometrics.

Algorithm 1: Data pre-processing
Input:
Raw IoMT Network Traffic Data (.pcap format)
List of Device MAC Addresses (device_MAC)
List of Desired Features (features_des)
Output: Modality-based Features (*.csv* format)
1. Utilize SplitCap Tool to extract device-related traffic for each MAC in device_MAC.
For each MAC, split the .pcap raw file and save it with the device name.
device_traf <- SplitCap(MAC)
2. Use CICFlowMeter Tool to extract statistical features (min, max, mean, std, variance) from device traffic.
IoT_features <- CICFlowMeter(device_traf)
3. Identify time-steps by counting packet repetition based on features: [”SrcBytes”, ”DistBytes”, ”SrcLoad”, ”DstLoad”, ”SrcGap”].
X <- groupcount(IoT_features, [”SrcBytes”, ”DistBytes”, ”SrcLoad”, ”DstLoad”, ”SrcGap”])
Store the top 'a' repetitions.
topa <- head(summary(X, ”GroupCount”), a)
4. Choose a common packet flow (e.g., 3).
if X == 3 then
IoMT_traf <- concatenate(IoT_features)
Assign the label.
IoMT_traf.Label <- Label
5. Separate datasets based on features_des.
Separate both the datasets and IoT_traf <- concatenate[IoMT_traf(1) IoT_traf(2)]
if IoT_traf.features == features_des(1) then
flow_metrics_rel_traf <- IoMT_traf(features_des(1))
else if IoT_traf.features == features_des(2) then
Biometrics_rel_traf <- IoMT_traf(features_des(2))

The methodology includes a description of the data preprocessing workflow for IoMT traffic data and patient biometrics in Algorithm 1. Before segmenting the data by device for focused analysis, the SplitCap tool is used to extract the raw network traffic data linked to particular device MAC addresses. The traffic is then thoroughly characterized by employing CICFlowMeter

to extract statistical features like mean, maximum, and standard deviation. Traffic can be grouped according to important characteristics such as SrcBytes and DstBytes to identify temporal patterns, separating common flows (e.g. 3). Packets containing recurring patterns. Labels e.g. 3. Are allocated, and features are divided into datasets specific to a given modality (e.g., network-flow metrics and patient biometrics; 0 for normal, 1). In order to handle uncertainty and improve interpretability, the last step uses fuzzy clustering, which enables soft assignments of data points to clusters.

The framework's efficient and modular design facilitates Its scalability. High-dimensional, multimodal datasets can be processed efficiently by the framework by utilizing sophisticated preprocessing tools and incorporating Bi-LSTM networks. Testing on the WUSTL-EHMS-2020 dataset in the real world shows its usefulness, as it achieves high accuracy in malware detection and anomaly prediction. Because of this, the framework is a useful tool for contemporary healthcare settings and can scale to larger datasets and a variety of IoMT applications while maintaining strong performance.

2.2 Fuzzy clustering in Feature Extraction with Stacked Bidirectional-LSTM Architecture

This proposed method is better at spotting suspicious activity by using different kinds of data and advanced techniques. It easily identifies the difference between normal and suspicious activity more accurately. It can work well in different situations and with different kinds of medical devices. It tackles various types of attacks and tricky situations effectively. It's like a well-rounded guard, ready to handle any security challenge that comes its way.

LSTM is a preferred method for evaluating multimodal longitudinal data since it is a reliable method for analyzing time-series data patterns. Bidirectional -LSTM, which is renowned for its exceptional ability to handle sequential data, is used to improve performance. Bidirectional -LSTM process input both forward and backward, giving them a more thorough grasp of context than unidirectional LSTMs.

For the study, five dual-layer Bidirectional-LSTM networks were trained independently to capture temporal trends within individual features and across different modalities. The outputs from these networks were then combined using a two-layer Bidirectional-LSTM network. Finding traits that various modalities shared in order to handle various types of data effectively was the aim of this integration. The four-layer bidirectional Stacked LSTM model used in this study consists of an input layer, two bidirectional LSTM layers (one with 64 neurons, one with 32 neurons), and an output layer with a single neuron. The learning rate, activation function, optimizer method, batch count, total number of epochs, and weighted initializer are the same tuning parameters for this model as they are for the stacking LSTM model. Figure 2 depicts the design of the suggested bidirectional LSTM. In this instance, bidirectional LSTM layers are used in place of regular LSTM layers.

The forward and backward Bi-LSTM outputs at each time step were concatenated to produce the Bidirectional LSTM's output. The final computation is an example of the Bi-LSTM's combined output. The method was efficient in handling individual modality data because the use of two layers did not add extra computation, even though the patient time series only had four steps. This method, which was inspired by Tran-Anh's 2022 work, enables the Bi-LSTM network to process various modalities efficiently and seamlessly.

$$f_{t_n} = \sigma(\theta_f \cdot \left[h_{t_{n-1}}, x_{t_n}\right] + b_f$$

$$i_{t_n} = \sigma(\theta_f \cdot \left[h_{t_{n-1}}, x_{t_n}\right] + b_i$$

$$\widetilde{C}_{t_n} = tanh(\theta_c \cdot \left[h_{t_{n-1}}, x_{t_n}\right] + b$$

$$C_{t_n} = (f_{t_n} \otimes C_{t_n} \otimes i_{t_n} \otimes \widetilde{C}_{t_n})$$

$$o_{t_n} = \sigma(\theta_o \cdot \left[h_{t_{n-1}}, x_{t_n}\right] + b_o$$

$$h_{t_n} = o_{t_n} \otimes tanh(C_{t_n})$$

$$y_n = \varphi(\theta_y \, h_{t_n} + b_y)$$

In a timeseries, the LSTM unit does not take into account the connection that exists between the previous input sequences and the current input sequences. In order to discover the inherent correlations that are present in a time series, the Bi-LSTM model combines two distinct hidden LSTM layers that are oriented in both the forward and backward directions.

$$\overrightarrow{h_{tn}} = \sigma(\theta_{\overrightarrow{h_n}} \cdot \left[h_{t_{n-1}}, \, x_{t_n}\right] + b_{\overrightarrow{h_n}}$$

$$\overleftarrow{h_{tn}} = \sigma(\theta^{h_n}{}_{\overleftarrow{t}} \cdot \left[\overleftarrow{h}_{t_{n-1}}, \, x_{t_n}\right] + b_{\overleftarrow{hn}}$$

$$\left(\overrightarrow{h_{t0}}, \, \overleftarrow{h_{t0}}\right) \ldots\ldots \left(\overrightarrow{h_{tn}}, \, \overleftarrow{h_{tn}}\right) = BiLSTM(X_{t0}, \, X_{t1}, \ldots\ldots\ldots X_{tn}$$

$$y_t = \sigma(\theta_{y_t} \, \overrightarrow{h_n} \, \overrightarrow{h_{tn}} + theta_{y_t} \, \overleftarrow{h_{tn}} + b_{yt})$$

The result of the Bi-LSTM y_t is then sent to the subsequent hidden layer. The output y_t from the layer that came before it is used as an input for the layer that comes after it in the design. In our analysis, the two Bi-LSTM layers need a pretty minimal amount of computing work. This is because the time series examined is rather brief.

2.3 Construction of stacked LSTM model

There are 4 layers in the Stacking LSTM architecture, with 32, 16, 16, and 1 neuron in each input layer, first and second LSTM layers, then the output layer, correspondingly. X, which contains attributes, is the input vector used by the model.

(v_t., u_t. u_{t-1}). Our output vector Y is featuring p t, the wind power, while feature set S(t) with past n observations is represented by v_{t-1}, ws_t. ws_{t-1}, wd_t. wd_{t-1}, and p_{t-n}. P_{t-1}. Following processing, the sequence is passed to the second LSTM layer, which uses the Rectified Linear Unit (ReLu) as its activation mechanism. Sending the anticipated sequencing to the output layer that is heavily linked is our final step. When the weight initializer variable is set to "Random Uniform," the model will start producing network weights with randomly generated, uniformly distributed values between 0 and 0.9. Root means square propagation (RMSprop) is one model optimizer that uses a learning rate of 0.001. A batch size of 32 and an epoch count of 5 are used to train the model. Figure 2 depicts the structure and flow of the stacked LSTM model.

To prevent CNNs from overfitting and improve their learning experience, this augmentation phase is essential. To the training split, several augmentation approaches are performed. The values of several augmentation techniques. The only photos that become enhanced are the ones used to train convolutional neural networks (CNNs), not the ones utilized for testing. In order to prevent too optimistic outcomes, this is done to make sure that the training and testing do not contain a copy of the picture. That is, at the beginning of each epoch, the model is fed randomly selected batches of the initial dataset, and the modifications are executed online. The pictures provided to the model at the end of each period also change depending on the changes used.

3 Results and Analysis

3.1 Evaluation metrics

A comprehensive analysis using a variety of evaluation metrics is essential when assessing deep learning models in practice. These metrics are essential for evaluating the efficacy and performance of multitask deep learning models. A variety of techniques can be used to give researchers and practitioners a thorough grasp of the model's capabilities, guaranteeing that a malevolent threat is aware of both its advantages and disadvantages. These assessment metrics are useful instruments for comparison, benchmarking, and decision-making when creating and improving machine learning techniques.

Accuracy:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} * 100$$

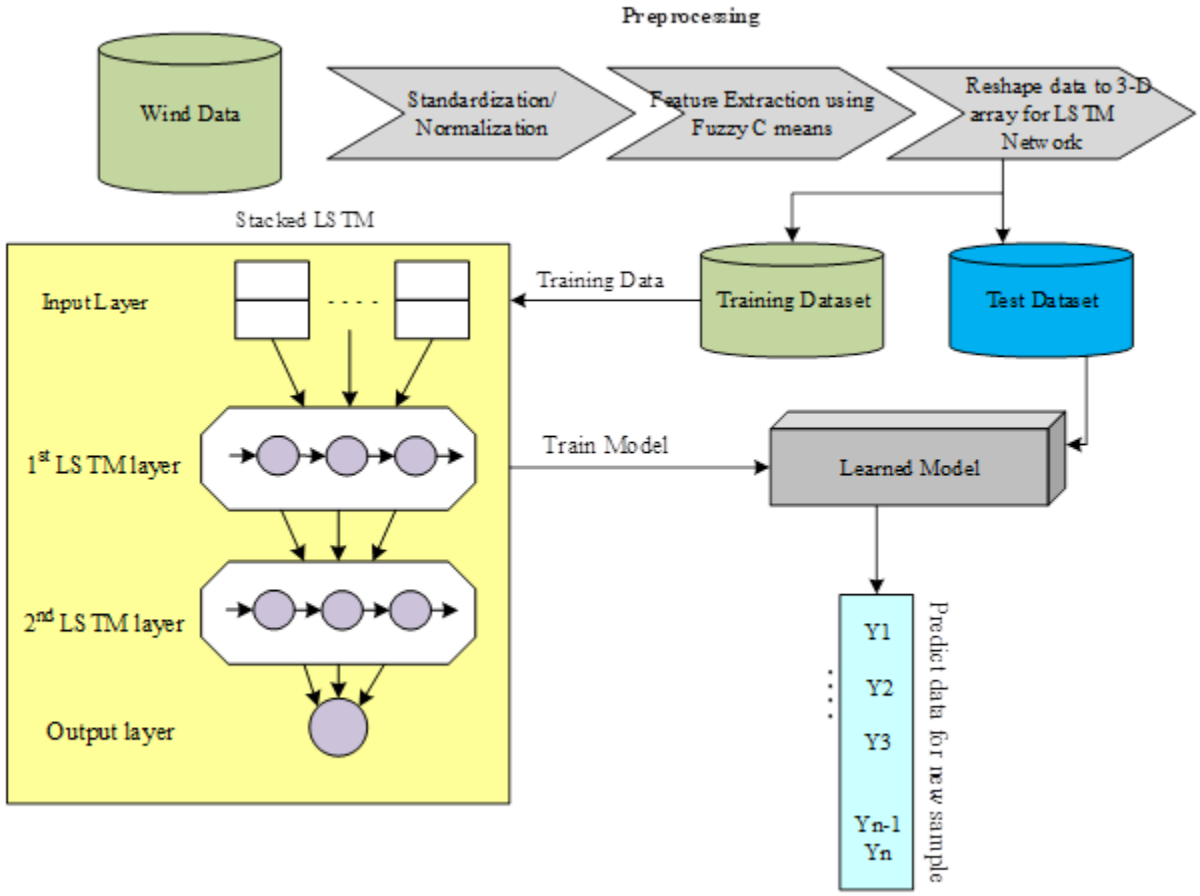

Fig 2. Duo Layered Bi-LSTM Architecture

Precision:

$$Precision = \frac{TP}{TP+FP} * 100$$

Recall:

$$Recall = \frac{TP}{TP+FN} * 100$$

F1-score.

$$F1-score = 2 \times \frac{Precision \times Recall}{Precision + Recall} * 100$$

3.2 NORMAL AND ABNORMAL HEART HEALTH

The dataset's normal and abnormal type cases' performance analyses were assessed using the suggested model. Table 1 displays the F-score values, recall, specificity, accuracy, and precision for the various normal and abnormal classes in the medical data classification. This stage one experiment evaluated two types of data to identify whether they were abnormal or normal. compares normal and abnormal heart health states using the proposed IoMT technique. Both the dataset from reference [3] and real-time sensor data exhibit exceptional accuracy when collected routinely. The study's ability to distinguish between normal and abnormal heart health conditions demonstrates the IoMT technique's potential for precise monitoring and diagnosis.

Table 1. The Bidirectional-LSTM technique is used to compare normal and abnormal class subjects

Datasets	Class	Accuracy	Precision	Recall	F1- Score
IoMT Real Time Sensor Dataset	Normal	96.85	95.10	97.04	95.23
Heart Disease Dataset		98.53	96.74	98.92	98.15
IoMT Real Time Sensor Dataset	Abnormal	98.31	96.48	98.83	97.98
Heart Disease Dataset		97.48	95.59	98.02	97.01

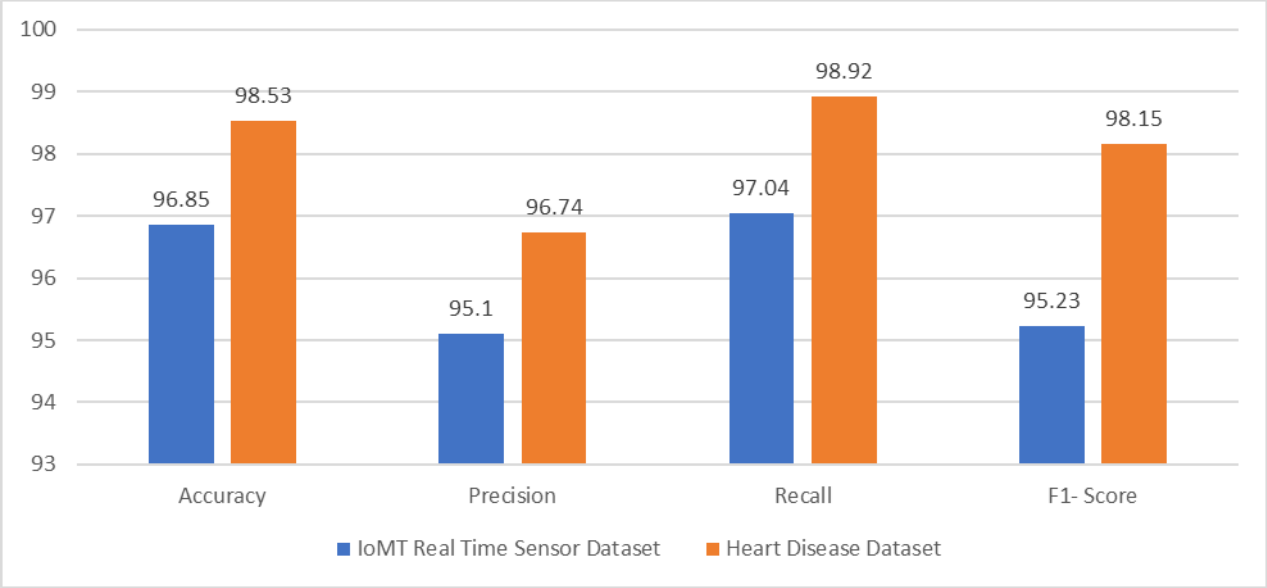

Fig 3. Bidirectional-LSTM technique for comparison of normal class subjects

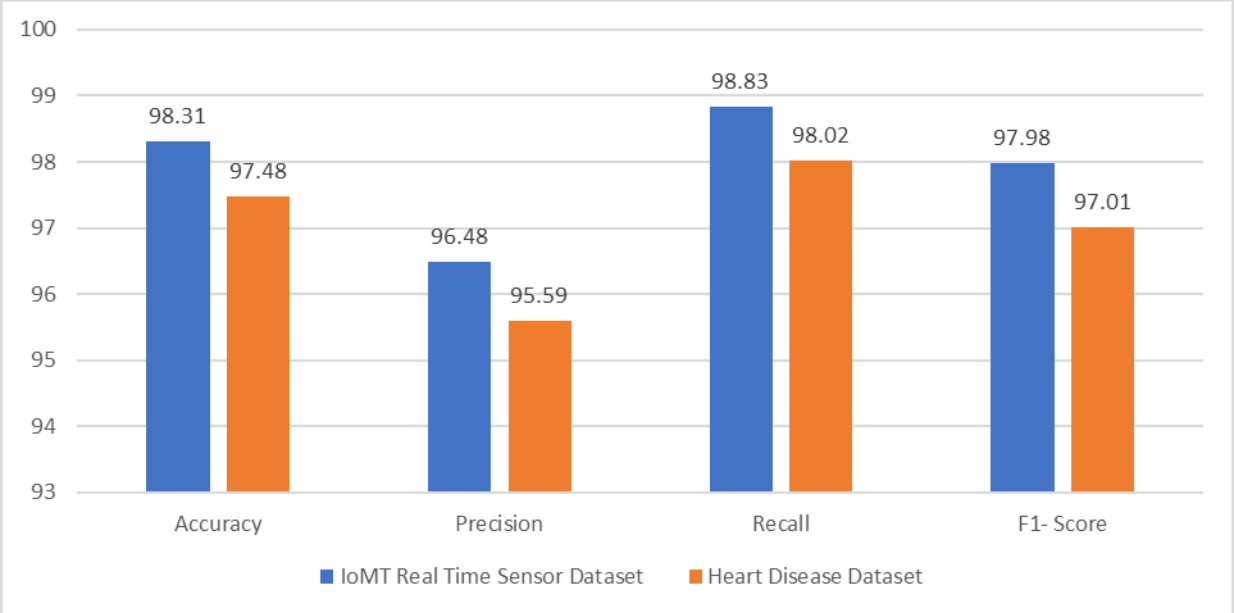

Fig 4. Bidirectional-LSTM technique for comparison of abnormal class subjects

The proposed Bi-LSTM model's accuracy, precision, recall, and F1-score were evaluated using these data. 96.85% accuracy, 95.10% precision, 97.04% recall, and 95.23% F1-score were attained by the suggested method in normal class classification using internet of medical things (IoMT) sensor data. In the heart disease datasets, the suggested approach obtained an F1-score of 98.15% for the normal cases, along with 98.53% accuracy, 96.74% precision, and 98.92% recall. Figures 5 and **??** display the performance of medical data classification graphically. The suggested approach obtained 98.3% accuracy, 96.48% precision, 98.83% recall, and 97.98% F1-score internet of medical things (IoMT) signal data picked up by sensors in the classification of abnormal classes. The suggested technical approach produced an accuracy of 97.48% percent, a precision of 95.59%, a recall of 98.02%, and an F1-score of 97.01% for the abnormal cases of the heart disease datasets.

3.3 Comparison and Discussion

Table 2. The compares recent research studies

Reference	Dataset's	Technique's	Accuracy
(Khalil, 2022)	EEG Signals	Convolutional Neural Network	77.78%
(Wang, 2022)	Computed Tomography	NB, LR, KNN	81%
(Wibowo, 2022)	Covid-19	RF, LR, SVM	88.43%
(Haque, 2022)	Diabetes, Parkinson	Deep Cad, Deep Neural Network	95.5%
(Kaur, 2022)	TCIA	Cukoo, Naive Bayes	98.61%
(Behera, 2023)	EEG Signals	WV-FLN	96.50%
S Manimurugan, 2024	EEG Signals	HLDA-MALO	97.50%
Proposed Model	WUSTL-EHMS	Fuzzy Clustering	92.00%
Proposed Model	WUSTL-EHMS	Bi-LSTM	98.53%

The comparative studies demonstrated a variety of machine learning methods with varying degrees of accuracy when applied to medical datasets. Using CNN on EEG signals, Khalil (2022) achieved an accuracy of 77.78%, indicating a moderate level of performance. In medical imaging, Wang (2022) showed strong results with ANN, LR, and NB, reporting 81% accuracy on CT images. For Covid-19 data, Wibowo (2022) achieved 88.43% accuracy using SVM, LR, and RF, demonstrating efficient model performance. Strong predictive capabilities were demonstrated by Haque (2022), who used Deep Cad and DNN to achieve 95.5% accuracy for diabetes and Parkinson's. Kaur (2022) showed remarkable performance by leveraging Cuckoo Search and Naive Bayes to achieve the highest accuracy of 98.61% on TCIA dataset. While S. Manimurugan (2024) achieved 97.50% accuracy using HLDA-MALO, Behera (2023) reported 96.50% accuracy using WV-FLN technique for EEG signals, demonstrating robust model effectiveness for EEG -Data. With accuracies of 92%, and 98.53%, respectively, our study using the WUSTL-EHMS approach with Fuzzy Clustering and Bi-LSTM demonstrated proficient performance despite the complexity of the datasets.

3.4 The Novelty of Work

The new Duo-Secure IoMT framework, which addresses critical vulnerabilities in Internet of Medical Things (IoMT) systems, is presented in this study. It combines cutting-edge machine learning techniques with sophisticated multimodal sensory computing. The framework specifically combines stacked bidirectional LSTM models with dynamic fuzzy clustering to enhance its detection capabilities and concurrently identify sophisticated cybersecurity threats like botnet-driven Distributed Denial of Service (DDoS) and zero-day attacks Predict abnormalities in heart health. Few studies currently in existence provide a thorough discussion of this dual function. The suggested framework shows creativity by using a two-stage methodology to continuously monitor and analyze IoMT traffic. It achieves remarkable accuracy rates of 92% in cardiac anomaly prediction and 98.5% in malware detection. The approach closes a significant gap in the current IoMT research, which usually concentrates on either network security or medical applications, but not both, by addressing cybersecurity and healthcare diagnostics. Additionally, by employing a robust dataset (WUSTL-EHMS-2020) and sophisticated preprocessing techniques, the study gets around significant drawbacks of conventional systems, like managing multimodal data and identifying intricate threats. This guarantees the model's scalability and efficacy in various IoMT contexts. With improved safety and diagnostic capabilities that are essential to the development of healthcare technology in the future, the suggested solution is a game-changing innovation for IoMT-based medical facilities.

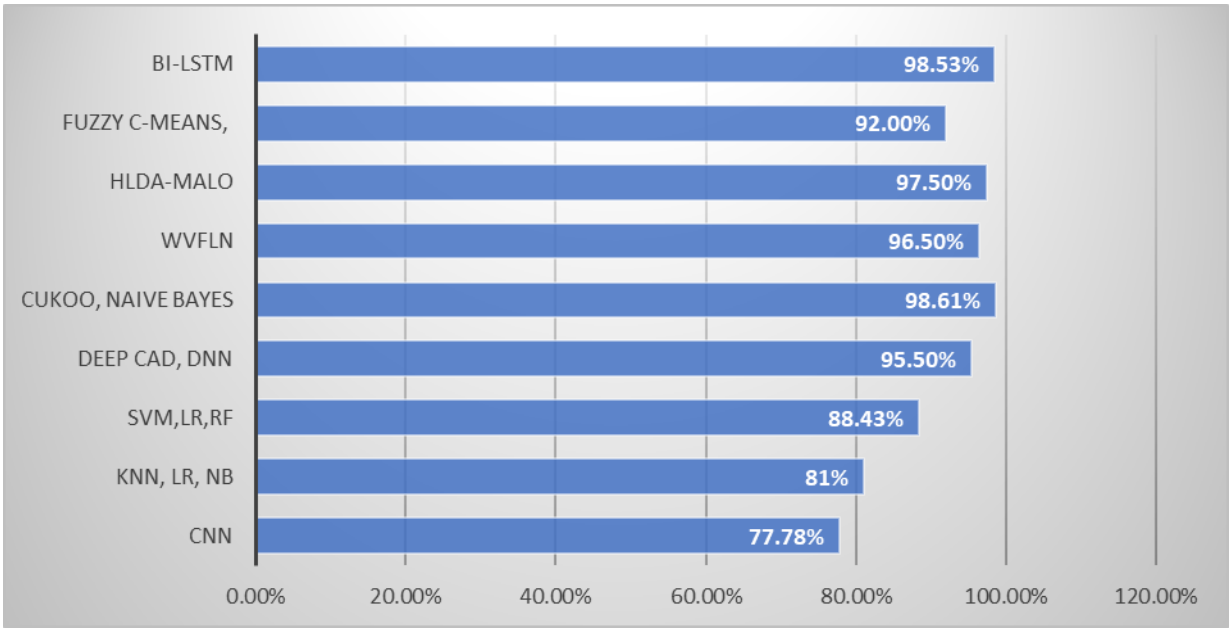

Fig 5. The comparison of recent research studies

4 Conclusion

The proposed approach manages anomalies and increases modelling training accuracy by selecting features and adjusting Bi-LSTM parameters. It achieves 98.50% accuracy in detecting network malware, making it a reliable tool for identifying potential security threats in IoMT infrastructure. Explainable AI may be used in future research to handle sensitive material with greater stability, interpretability, and fairness. Given the growing need for virtual care monitoring systems, possible drawbacks like battery and computer power limitations are acknowledged. Future research will concentrate on improving techniques by adjusting hyperparameters, constricting the feature space, enhancing model complexity, and investigating complex attack scenarios. Furthermore, it is suggested that Explainable Artificial Intelligence (XAI) techniques be used to increase anomaly detection's transparency with the ultimate goal of increasing accuracy and efficiency.Non-Cited References [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20]

References

1) Miotto R, Wang F, Wang S, Jiang X, Dudley JT. Deep Learning for Healthcare: Review, Opportunities and Challenges. *Briefings in Bioinformatics*. 2018;19:1236–1246. https://doi.org/10.1093/bib/bbx044.
2) Jabeen F, Maqsood M, Ghazanfar MA, Aadil F, Khan S, Khan MF, et al. An IoT Based Efficient Hybrid Recommender System for Cardiovascular Disease. *Peer-to-Peer Networking and Applications*. 2019;12:1263–1276. https://doi.org/10.1007/s40846-018-0421-y.
3) Huang J, Wu X, Huang W, Wu X, Wang S. Internet of things in health management systems: A review. *International Journal of Communication Systems*. 2020;34. https://doi.org/10.1002/dac.4683.
4) Lin J, Fu R, Zhong X, Yu P, Tan G, Li W, et al. Wearable sensors and devices for real-time cardiovascular disease monitoring. *Cell Reports Physical Science*. 2021;2:1–25. https://doi.org/10.1016/j.xcrp.2021.100541.
5) Rahaman A, Islam M, Islam R, Sadi MS, Nooruddin S. Developing IoT Based Smart Health Monitoring Systems: A Review. *Revue d'Intelligence Artificielle*. 2019;33:435–440. https://doi.org/10.18280/ria.330605.
6) Panicker S, P G. Use of Machine Learning Techniques in Healthcare: A Brief Review of Cardiovascular Disease Classification. *2nd International Conference on Communication & Information Processing (ICCIP) 2020*. 2020. http://dx.doi.org/10.2139/ssrn.3681833.
7) Rana A, Prajapat S, Kumar P, Gautam D, Chen C. Designing a Security Framework Based on Hybrid Communication in Internet of Nano Things. *IEEE Internet of Things Journal*. 2024;11:7265–7284. https://doi.org/10.1109/JIOT.2023.3315712.
8) Raj A, Sharma V, Rani S, Shanu AK, Kumar N. Strengthening the Security of IoT Devices Through Federated Learning: A Comprehensive Study. *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 2024;p. 1–5. https://doi.org/10.1109/ICRITO61523.2024.10522388.
9) Rashad M, Hussein DL, Abdalkarim HD, Azeez R. Future IoT Software in Healthcare Also Exploring IoT Industry Application. *UHD Journal of Science and Technology*. 2022. https://doi.org/10.21928/uhdjst.v6n1y2022.pp70-75.
10) Zheng W, Cao Y, Tan H. Secure sharing of industrial IoT data based on distributed trust management and trusted execution environments: a federated learning approach. *Neural Computing and Applications*. 2023;35:21499–21509. https://doi.org/10.1007/s00521-023-08375-6.

11) Jhaveri RH, G TR, Clark AC. Preface to the Special Issue on Privacy and Security for Internet of Things. *International Journal of Wireless Information Networks*. 2022;29:405–406. https://doi.org/10.1007/s10776-022-00588-1.
12) Zolanvari M, Yang Z, Khan KM, Jain R, Meskin N. TRUST XAI: Model-Agnostic Explanations for AI With a Case Study on IIoT Security. *IEEE Internet of Things Journal*. 2022;10:2967–2978. https://doi.org/10.1109/JIOT.2021.3122019.
13) Regan R, Jayashree J, Kurmitha M. Smart Distributed Multi-Ledger Construction Algorithm for Internet of things (IoT). *International Journal of Engineering and Computer Science*. 2022;11(07):25543–25548. https://doi.org/10.18535/ijecs/v11i07.4679.
14) Zeng Q, Naït-Abdesselam F, Chen Z. A HITL-Integrated Machine Learning Approach to Secure Drone Networks for IIoT Applications. *2023 IEEE Globecom Workshops (GC Wkshps)*. 2023;p. 614–619. https://doi.org/10.1109/GCWkshps58843.2023.10465098.
15) Bagchi P, Bera B, Das AK, Shetty S, Vijayakumar P, Karuppiah M. Post Quantum Lattice-Based Secure Framework using Aggregate Signature for Ambient Intelligence Assisted Blockchain-Based IoT Applications. *IEEE Internet of Things Magazine*. 2023;6:52–58. https://doi.org/10.1109/IOTM.001.2100215.
16) Kumar R, Kumar P, Jolfaei A, Islam AN. An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications. *2023 IEEE International Conference on Consumer Electronics (ICCE)*. 2023;p. 01–06. https://doi.org/10.1109/ICCE56470.2023.10043450.
17) Kumar A, Sharma I. Augmenting IoT Healthcare Security and Reliability with Early Detection of IoT Botnet Attacks. *2023 4th International Conference for Emerging Technology (INCET)*. 2023;p. 1–6. https://doi.org/10.1109/INCET57972.2023.10170738.
18) Golec M, Golec M, Xu M, Wu H, Gill SS, Uhlig S. PRICELESS: Privacy enhanced AI-driven scalable framework for IoT applications in serverless edge computing environments. *Internet Technology Letters*. 2024 Feb. https://doi.org/10.1002/itl2.510.
19) Kumar R, Malik A, Ranga V. Security concerns over IoT routing using emerging technologies: A review. *Transactions on Emerging Telecommunications Technologies*. 2023;34(15). https://doi.org/10.1002/ett.4798.
20) Sedik A, Faragallah OS, El-sayed HS, Banby GM, El-Samie FE, Khalaf AA, et al. An efficient cybersecurity framework for facial video forensics detection based on multimodal deep learning. *Neural Computing and Applications*. 2021;34:1251–1268. https://doi.org/10.1007/s00521-021-06416-6.