Journal of Computer Applications and Information Technology
Vol. 1, Issue. 3, Sep 2025, pp. 1~12
ISSN: 3107-6424

Edge-Driven Machine Learning for Real-Time Health Anomaly Detection in IoT-Based Healthcare: A Modular Framework

Dr. Christhu Raj M R[1], Sangwoo Jeon[2]
[1]Directorate of Learning and Development,
SRM Institute of Science and Technology, Kattankulathur, India. christhm1@srmist.edu.in
[2]Department of Computer Science and Engineering, Konkuk University, Seoul, South Korea.
jswp5580@konkuk.ac.kr

Article Info

Article History:

Received Jul 11, 2025
Revised Aug 10, 2025
Accepted Sep 07, 2025

Keywords:

Healthcare IoT
Real-time Anomaly Detection
Edge-driven Machine Learning
Patient Monitoring
Data Security

ABSTRACT

The rapidly expanding field of healthcare IoT has the potential to transform patient monitoring and intervention. Real-time anomaly detection is necessary to safeguard patient information and device integration in light of these new security threats brought about by this interconnectedness. Integrating the Internet of Things (IoT) into healthcare enhances patient care while also improving the performance and reliability of healthcare delivery system. Ethical concerns, interoperability, and data security must be resolved if the benefits of IoT in healthcare are to be fully realized. Patients' health data is measured by IoT devices on a regular basis and shared with a server for additional analysis. Various machine learning (ML) approaches are employed on the server to help with early disease identification and to send out alerts when vital signs deviate from normal. IoT devices regularly measure patient health data and send it to a server for further analysis. The server employs a variety of ML techniques to assist in the early detection of diseases and to notify users when vital signs diverge from normal. Patient health data is routinely measured by IoT devices and sent to a server for additional analysis. The server uses a range of edge-driven ML models to alert users when vital indicators deviate from normal to anomaly identification. In this study, we introduce an edge-driven ML for real-time health anomaly detection in IoT-based healthcare: a modular framework (EDML-RHADIOTF). The EDML-RHADIOTF involves data preprocessing, feature extraction and anomaly classification. In comparison to previous solutions, the suggested EDML-RHADIOTF model shown an outstanding enhancement in anomaly detection based on an analysis of its performance outcomes. With a 96.55% accuracy rate in both reduced and full feature space, SVM performed better across anomaly classification of IoT attacks. A reduction in computing response time, which is necessary for quick response and real-time attack detection, complemented this improvement.

Corresponding Author:

Dr. Christhu Raj M R,
Directorate of Learning and Development,
SRM Institute of Science and Technology, Kattankulathur, India.
Email: christhm1@srmist.edu.in

1. INTRODUCTION

One significant technological advancement that forms the foundation of numerous future applications in the domain of health care is the Internet of Things (IoT). The IoT uses a variety of sensors to collect data about people, things, and the environment. Because of the frequent transmission of this data to the cloud server, application managers are able to take a variety of actions to increase the effectiveness of their programs [1]. In a similar vein, AI methods can be applied to autonomously manage the apps according to the information gathered. Finding anomalous patterns or behaviors in data flows produced by IoT sensors is crucial [2], particularly in industries like agriculture and education that heavily depend on IoT technology. The smooth integration of devices in various sectors produces a significant volume of data that promotes innovation and increases operational effectiveness.

However, as the volume of data increases, these fields are also exposed to potential vulnerabilities, which highlights how important it is to spot unusual or inappropriate patterns in order to maintain integrity and guarantee security. By employing advanced anomaly detection techniques, educators and agricultural professionals may safeguard against malicious actions, deviations, and abnormalities that could cause system disruptions or compromise sensitive information [3].

This procedure not only ensures that edge-driven operations are reliable, but it also highlights how important anomaly detection is to bolstering the foundational elements of agriculture and education. This makes it possible for these industries to achieve operational excellence and preserve data integrity while successfully utilizing the benefits provided by IoT technology.

One significant use of edge driven technology is in healthcare, where patients are given wearable gadgets to gather vital information. Body measurements like blood pressure, heart rate, oxygen level, sugar level, etc., could be examples of this type of data [4] is therefore a significant use case that has a profound effect on people's lives.

Designing effective methods to ensure that data recording and sharing are dependable and secure is essential since IoT-enabled health care entails the recording and exchange of key data associated with the human security. Numerous security breaches can affect healthcare systems, which can cause users to lose faith in the information they receive. IoT-enabled healthcare apps may fail as a result of incorrect decisions made in a number of situations involving harmful data [5].

Healthcare systems are susceptible to a various privacy risks, involving DoS attacks, in which malevolent individuals attempt to prevent the wearable from sharing data with the cloud [6]. This can be accomplished by sending the wearable inaccurate data frequently or by preventing it from connecting to the wireless media. In a similar vein, spoofing is another prevalent cyberattack when malevolent actors conceal their identities in order to obtain victims' vital health information [7]. Brute force attacks, which attempt to crack the password of users' wearable devices and obtain sensor data, are another type of cyberattack [8]. The dependability of IoT health care apps can also be lowered by a variety of other assaults, including data integrity and eavesdropping.

Hospitals can take into consideration the widely used IoT architecture. There are primarily three kinds of components in such an architecture:

- IoT nodes are made up of various sensors, gateways, network medical equipment, and remote care resources. To the closest gateway, sensors will transmit various kinds of data and information, such as staff and patient information, the condition of medical equipment, etc [9].
- An edge router, also known as a border router, is a type of specialized router that sits at a network's edge or boundary. This node makes ensuring that its network is connected to external networks, such as the Internet or a wide area network.

- The edge router interconnects with the distant networks and cloud services via an external border gateway protocol, which is more commonly exploited over the Internet. The edge router can be used to notify the right users and perform analysis activities.
- Database and visualization module: this module serves as the network's terminal and houses all of the data gathered from the various network nodes. To improve the healthcare system and guarantee patient safety, data is presented to users according to their roles. Both local networks and cloud servers may house the database and visualization module [10].

By transporting computing power nearer to information sources, edge-driven intelligence (EDI) is revolutionizing data pre-processing, analysis, and decision-making in the modern day. Security and privacy will remain high concerns, requiring the deployment of enhanced edge security measures to protect sensitive data and reduce cyber risks. By developing edge-native programs tailored to specific edge configurations and resource usage in EDI systems, performance will be optimized. Edge-driven ML has the potential to completely transform a number of fields and industries in the future. Organizations can fully utilize EDI to open up new possibilities and accomplish sustainable evolution in the digital age by embracing emerging trends, tackling related obstacles, and utilizing opportunities. Healthcare businesses can proactively identify and address security threats before they jeopardize the integrity of health records by utilizing ML-based IDS at the edge.

Problem Statement and Assumptions

Radio interfaces in hospital infrastructures allow nodes to communicate vast amounts of sensitive data. For precise event detection and decision-making, these data must be safeguarded. For instance, protecting patient privacy is necessary to stop identity theft and illegal identification. Furthermore, because so many patients are in trying circumstances, the hospital structure itself is delicate. Therefore, keeping the building stable and safeguarding it from various anomalous events is a challenge in and of itself. For instance, a patient in an operating room may suffer injury if their temperature rises or falls. Data that deviates from typical patterns is typically considered an anomaly. There are two categories of anomalies in the context of smart hospitals: data anomalies connected to e-health and abnormalities related to IoT networks. Events like fires (strange humidity temperature and data), variations in patient conditions (weird heartbeat rates), etc., can produce anomalies in e-health data. Particularly for hospital infrastructures, these anomalies are extremely important and need to be identified in real time without sending out false alarms. On the other hand, anomalies in IoT are normally defined by an odd shift in network traffic and node behavior.

They are mostly caused by node failures and network attacks. In order to maintain data accuracy and prevent issuing false alarms, experts now consider this kind of anomaly to be a top priority task. The analysis task may be performed on cloud servers or on a local network for the purpose of anomaly identification.
Nonetheless, the data handled by smart healthcare systems is extremely important and sensitive to latency. In actuality, the danger of security breaches may rise when data is sent to cloud servers for analysis and decision-making. Additionally, depending on the available bandwidth and processing power, this could result in an additional delay in data transmission.

Nevertheless, the data that intelligent healthcare systems handle is crucial and latency-sensitive. Additionally, this can cause an extra delay in data transmission, contingent on the processor power and available bandwidth.

- By using ML methods on an unbalanced dataset, the authors were able to create models with high accuracy and low precision scores. The goal of the study is to balance the dataset such that ML algorithms are trained appropriately.
- To assess supervised machine learning methods on the balanced dataset using both binary (2-Class) and multiclass (8 and 34-Class) representations.
- To use feature reduction to assess machine learning models' computational response times. To ascertain which characteristics are necessary for machine learning models to generalize.

In this work, we introduce an edge-driven machine learning for real-time health anomaly recognition in IoT-based healthcare: a modular framework (EDML-RHADIOTF). The EDML-RHADIOTF involves data preprocessing, feature extraction and anomaly classification. In comparison to previous solutions, the suggested EDML-RHADIOTF model shown an outstanding enhancement in anomaly detection based on an analysis of its performance outcomes. With a 96.55% accuracy rate in both reduced and full feature space, SVM performed better across anomaly classification of IoT attacks. A reduction in computing response time, which is necessary for quick response and real-time attack detection, complemented this improvement.

2. RELATED WORK

[11] Offers a unique security architecture that combines SVM and Hidden Markov Models (HMM) to accurately identify anomalies in real-time healthcare IoT applications. Real-time efficiency and strength are given top priority in the framework. Wearable, medical, and other Internet of Things sensor data is meticulously divided into time periods. Each segment's features, such as statistical summaries, patterns, and frequency domain characteristics, are meticulously extracted. Accurate anomaly detection requires feature engineering. The foundation of the framework is the integration of HMM and SVM capabilities. HMM analyzes patterns of change over time and properly depicts hidden states inside segmented data sequences. Each state is then examined using an independent-trained SVM. This SVM can distinguish between normal and anomalous data points based on their proximity to a decision hyperplane in feature space. This technique increases sensitivity to aberrant patterns and decreases false positives by combining SVM classification performance with HMM temporal capabilities. Comprehensive tests on the PhysioNet Challenge 2017 dataset, which consists of a variety of ECG records with identified abnormalities, demonstrate the framework's outstanding performance. With maximum accuracy, HMM-SVM beats Naive Bayes, RF, and LSTM. Additionally, the framework's demonstrate its sophisticated ability to identify genuine anomalies and minimize false alarms. In addition to its exceptional accuracy, the framework places a high priority on real-time comprehension and application. By exposing context and potential reasons for anomalies, HMM-SVMs uncover concealed data state changes. Real-time functionality may be seamlessly integrated into low-resource IoT devices thanks to modular architecture and effective algorithms, facilitating prompt and efficient security responses. In summary, an HMM-SVM framework for quick healthcare IoT anomaly detection is presented in this study. The framework achieves excellent accuracy while emphasizing understandability and real-time applicability. This architecture can strengthen device security, safeguard patient data, and provide a more dependable healthcare IoT ecosystem.

[12] Use the IoT dataset to train machine learning methods for effective anomalous network traffic identification. There are various f IoT assaults in the dataset, which are considered into seven major groups. The current study generates non-biased supervised machine learning models using a pre-processed dataset and a balanced representation of classes. By removing strongly correlated characteristics, decreasing dimensionality, minimizing overfitting, and expediting training periods, these models are further examined. With a highest accuracy rate in both reduced and full feature space, Random Forest was found to perform best across binary and multiclass categorization of IoT attacks. A decrease in computing response time, which is necessary for real-time attack detection and response, complemented this improvement.

To automatically measure cardiovascular activity, an intelligent end-to-end system for anomaly detection and categorization of raw, one-dimensional (1D) ECG signals is provided by [13]. Before being stored in the cloud, the obtained raw ECG information is meticulously preprocessed and then thoroughly examined for anomalies. An auto-encoder (AE) technique based on deep learning is used to detect anomalies in 1D-ECG time-series signals. The implemented system then uses a multi-class classification technique to identify it. The big and varied datasets' enhanced feature-engineered parameters have been included to increase the model's robustness and classification accuracy. For a cohesive solution, cloud-based storage and machine learning capabilities from Amazon Web capabilities (AWS) have been used for the training. Raw ECG signal multi-class classification is difficult since there are many possible label combinations and noise sensitivity. In order to address this issue, an

enhanced feature-engineered dataset is used to compare the classification accuracy of a wide range of machine methods. In order to reduce computation, the suggested method uses wavelet temporal scattering features to reduce the raw signal size by up to 95%. The findings demonstrate that the long short-term memory (LSTM) approach outperformed various cutting-edge methods in terms of classification accuracy, achieving 100% and an F1 score on the three-class test dataset.

[14] Demonstrated how to use biomedical sensors to construct an AI-edge healthcare system based on the Internet of Things. In order to determine the most accurate method for real-time raw signals, this paper also attempts to analyze cloud data obtained through biomedical sensors using signal analysis for anomaly detection. The real-time processing speed was increased by achieving 95% signal reduction with the use of wavelet time scattering feature extraction. LSTM autoencoders reach 98% accuracy in real-time signal anomaly detection.

[15] Uses a dataset of 200,000 records to present a machine learning-driven system for (1) detecting malicious cyberattacks and (2) recognizing malfunctioning device anomalies. Supervised learning (XGBoost, K-Nearest Neighbors (K-NN)), semi-supervised learning (Generative Adversarial Networks (GAN), Variational Autoencoders (VAE)), and unsupervised learning (One-Class Support Vector Machine (SVM), Isolation Forest, Graph Neural Networks (GNN), and LSTM-AE) are the three learning approaches used to evaluate eight machine learning models. Numerous measures, including F1-score, precision, recall, accuracy, ROC-AUC, and computing efficiency, were thoroughly evaluated. Isolation Forest successfully struck a compromise between precision and recall, while XGBoost reached highest accuracy for anomaly detection with a low computational overhead (0.04s). With increased latency and decreased accuracy, LSTM-AE fared poorly. With the lowest accuracy and ROC-AUC, GAN displayed the highest computational cost. By using efficient anomaly detection techniques, these discoveries optimize the IoT-enabled healthcare security. This framework has the potential to prevent data breaches, reduce system downtime, and guarantee the continuous and secure operation of medical devices by enhancing early detection of cyber threats and device failures. In the end, this could protect patient health and confidence in IoT-driven healthcare solutions.

[16] Examines just one important IoT health care security issue, for which improvements in threat detection and response were investigated using a novel security architecture based on RNNs. This method used RNNs to progressively simulate network traffic and device behavior in order to detect anomalies and possible breaches. As a result, we present the RNN-based model together with an all-inclusive security architecture that includes real-time monitoring tools, authentication procedures, and data encryption. In comparison to conventional security solutions, experimental results demonstrate that our RNN-based architecture dramatically enhances harmful activity identification and lowers false positives. A robust, scalable, and flexible security solution that is suited to the dynamics of the IoT healthcare setting would be offered by the suggested model. These results may show how RNNs might improve IoT security and offer fresh approaches to creating safer and more effective healthcare systems.

3. THE PROPOSED METHODOLOGY

In this study, we introduce an EDML-RHADIOTF technique. The EDML-RHADIOTF involves data preprocessing, feature extraction and anomaly classification. In comparison to previous solutions, the suggested EDML-RHADIOTF model shown an outstanding enhancement in anomaly detection based on an analysis of its performance outcomes. A reduction in computing response time, which is necessary for quick response and real-time attack detection, complemented this improvement.

3.1. Data Pre-processing

The three primary stages of this phase are normalization, missing value handling, and data cleansing. The mean value is used to replace missing numbers, and the mode is used to replace missing nominal values. One-hot encoding transforms categorical input into numerical representation [17]. By applying the min-max technique, numeric values are normalized to fall between 0 and 1.

These careful procedures are implemented to guarantee that the data is appropriately processed for additional analysis and modeling, leading to more accurate and dependable results.

$$Xnorm = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

Numerical values are standardized within the range of 0 to 1 using the min-max procedure, which is described in Eq. 1. This makes it easier to compare various variables.

3.2. Feature Extraction Using PCA

The primary elements that characterize the healthcare information in the feature space were extracted at this stage by using the PCA approach to each node. After gathering enough sensor data, this phase was completed offline.

The logistic regression approach [18], which can differentiate between normal and anomalous healthcare information, was used to train the detection model after the PCA-extracted features were fed into a ML classifier. Since the method is computationally light and doesn't require any complex processes, the similar technique was used online.

After the PCA-extracted features were fed into a ML classifier, the recognition method was trained using the logistic regression technique, which can discriminate among normal and anomalous healthcare information. The same procedure was employed online since the method doesn't require any complicated processes and is computationally light.

Input: Information gathered from sensors

Output: The data's classification as either normal or abnormal

1: Gather sensor data.

2: Perform standardization and normalizing of data

3: Take the data's raw features and extract them.

4: Utilize PCA on the unprocessed data and attributes.

5: Choose the optimal n eigenvector for the PCA features.

6: feed the logistic regression classifier with the chosen PCA features.

7: read the sensor's most recent measurement (data).

8: Utilize PCA on recently acquired data.

9: Provide the classifier with data that includes PCA features.

10: The measurement's normality or anomaly will be determined by the classifier.

Apply feature standardization to the data, which assigns a zero-mean and unit-variance to each feature's values. It significantly impacts PCA. because the covariance matrix may be impacted by scaling. A correlation analysis is conducted by doing an element-wise multiplication between two features. Therefore, the covariance matrix will serve different purposes if the two characteristics are not scaled with the same range. The data has undergone normalization, or feature scaling, following the CNN's extraction of 512 features. Equation 1 has been utilized in its execution.

$$x' = \frac{x - \overline{x}}{\sigma} \quad (2)$$

Where σ is the standard deviation, x is the original feature vector, and X is the feature vector's mean. Let Z be the feature matrix X in its standardized form.

2) The matrix A=Z·Z^T has been used to determine the covariance matrix for this investigation.

3) The eigenvalue and eigenvector have been determined following the computation of the covariance matrix. Compute eigenvalues through (A-λI)=0 and eigenvector by the solution of (A-λI)V=0 for various lambda values. Each eigenvector in this study has 512 items, and there are 512 eigenvalues.

4) The eigenvalues and corresponding eigenvector are then sorted in descending order. The top 100 eigenvalues are chosen from the 512 eigenvalues.

5) Multiply the eigenvector matrix, E, by the feature matrix, X [19].

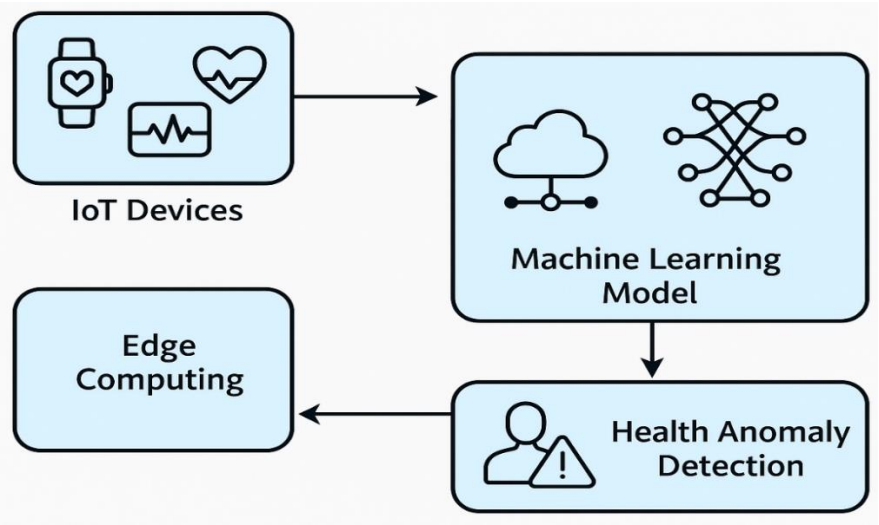

Figure 1. Working flow of the EDML-RHADIOTF mode

3.3. SVM based Anomaly detection

The presented SVM anomaly recognition method detects anomaly behavior in the network by determining the typical activity and using it as a baseline. Consequently, any deviation from that baseline is seen as abnormal.

The SVM was used to solve categorization problems. The non-linear SVM can capture complex correlations between parameters without the need for difficult transformation when multiple parameters are included. The concept behind SVM is simpler: the algorithm generates a hyperplane or line that splits information into normal and abnormal classes. It uses a mathematical function known as the kernel to reformulate data.

After this adjustment, the SVM algorithm defines an optimal border between the labels. It primarily makes a number of adjustments to split the dataset based on the specified labels or outputs.

$$H(n,N) = [{}^{h}_{h_{(n,1)}} h_{(3,\ldots'1)} h_{(2,1)}(1,1) h_{(n,2)} h_{(3,\ldots'2)} h_{(2,2)} h(1,2) \ldots h_{(n,N)} h_{(1.'N)]} h_{(1.'N)} h(1.'N) \quad (4)$$

Lastly, the Moore-Penrose pseudo inverse is used to get the output layer weight $\beta_{(N,t)}$.

$$\beta_{(N,t)} = H^{\uparrow}_{(N',\, n)} T_{(n,t)} \quad (5)$$

Where T =Output of training dataset and t =amount of outputs. Temporal dependencies are taken into account. Segments are classified as normal or anomalous by the SVM model after it has been trained for the state. When anomalies are found, alert systems notify medical staff and initiate additional research or action. This framework is mathematically sound and effective. It employs SVM and HMM to identify irregularities instantly [20].

4. RESULTS AND DISCUSSION

In this section, real-time anomaly detection outcomes of the EDML-RHADIOTF method are tested under various datasets. The feature extraction process can be done by PCA layer and classification was performed through the SVM model. We evaluated the performance of all models using dissimilar performance metrics. In Table 1, precision, recall, AP, and mAP values of EDML-RHADIOTF, YOLOv10, CNN, and Bi-LSTM are compared. In addition, the outcomes assured that the EDML-RHADIOTF outperforms other existing techniques.

Table 1. Comparative outcomes of EDML-RHADIOTF with other existing models

Models	Precision (%)	Recall (%)	AP (%)	mAP (%)
EDML-RHADIOTF	83.20	93.64	94.20	96.20
YOLOv10	73.11	79.62	91.46	84.36

CNN	79.05	83.25	89.40	84.36
Bi-LSTM	89.65	82.50	90.32	89.23

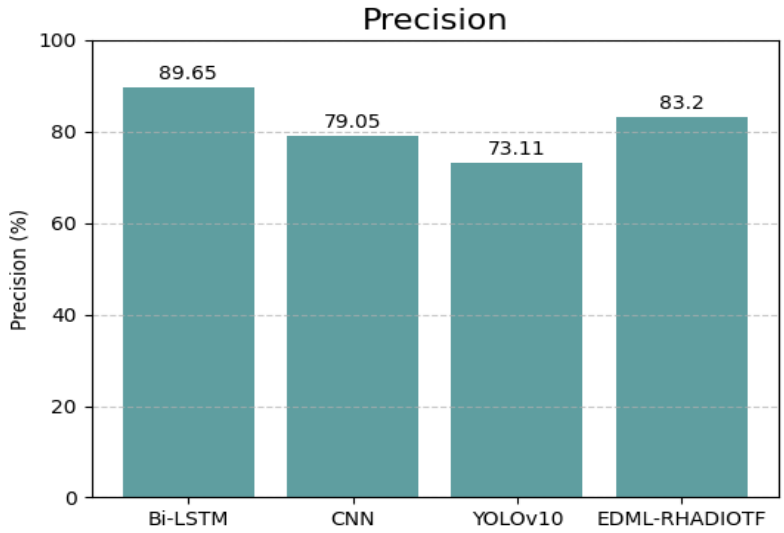

Figure 2. Precision of EDML-RHADIOTF with other existing techniques

Figure 2 demonstrates the anomaly detection outcomes EDML-RHADIOTF with YOLOv10, CNN, and Bi-LSTM approaches. The simulation results implied that the CNN and YOLOv10 models have reported lesser precision values of 79.055 % and 73.11%. We compare the detection performance of all the models in Table 2. Subsequently, the Bi-LSTM technique has obtained moderate precision value of 89.65%. However, the proposed EDML-RHADIOTF method achieves highest performance with a precision value of 90.6 % compared to other techniques.

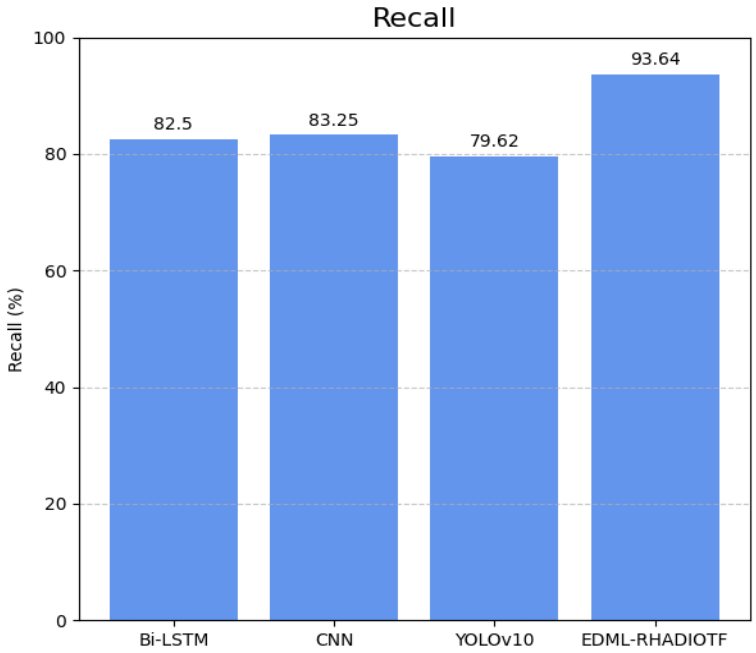

Figure 3. Recall of EDML-RHADIOTF with other existing techniques

The simulation analysis of EDML-RHADIOTF with YOLOv10, CNN and BiLSTM methods is illustrated in Fig. 3 and Table 2. The simulation values indicated that the YOLOv5 model has reported highest precision values of 80.2%. Subsequently, the YOLOv8 and YOLOv10 models have gained moderate precision values of 73.4 % and 72.5%. However, the proposed method YOLOv10 achieves minimum performance with a recall value of 72.5 % compared with YOLOv5 model.

Table 2. Anomaly detection outcomes of EDML-RHADIOTF with other existing models

Models	**Recall (%)**
EDML-RHADIOTF	93.64
YOLOv10	79.62
CNN	83.25
Bi-LSTM	82.50

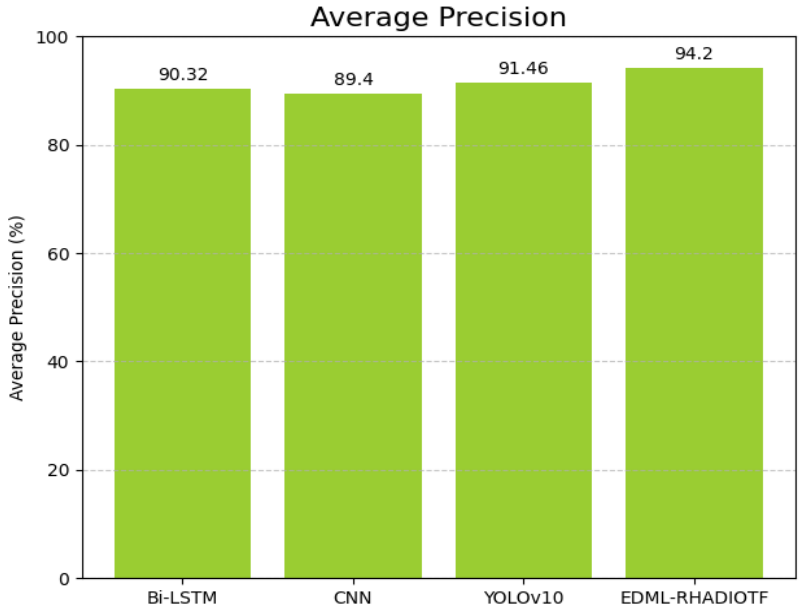

Figure 4. Average precision of EDML-RHADIOTF with other existing techniques

Figure 4 and Table 3 illustrates the experimental analysis of EDML-RHADIOTF with YOLOv10, CNN and BiLSTM approaches. The simulation results implied that the Bi-LSTM and YOLOv10 have reported moderate precision values of 90.32 % and 91.46%. Subsequently, the CNN model has obtained lesser precision values of 89.40 %. Simultaneously, the proposed EDML-RHADIOTF method achieves highest detection accuracy with a precision value of 94.20 % compared to other YOLOv10, CNN and BiLSTM approaches methods.

Table 3. Anomaly detection outcomes of EDML-RHADIOTF with other existing models

Models	**AP (%)**
EDML-RHADIOTF	94.20
YOLOv10	91.46
CNN	89.40
Bi-LSTM	90.32

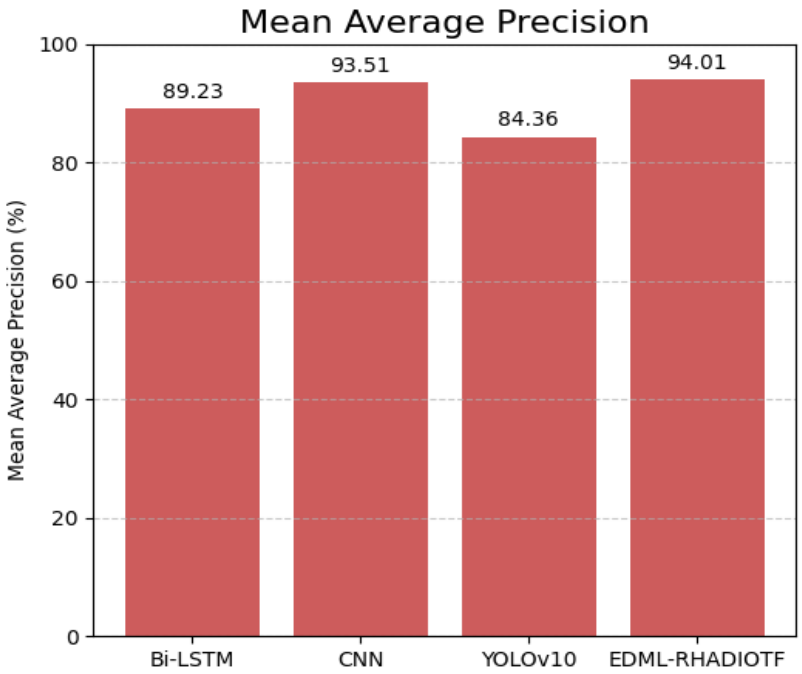

Figure 5. Mean average precision of EDML-RHADIOTF with other existing techniques

Figure 5 and Table 4 demonstrate the mAP analysis EDML-RHADIOTF with other YOLOv10, CNN and BiLSTM techniques. The simulation results implied that the Bi-LSTM attained lowest mAP value of 89.23%. YOLOv10 and CNN have reported moderate precision values of 84.36% and 84.36%. However, the proposed EDML-RHADIOTF model obtained maximum performance with a precision value of 96.20% compared to YOLOv10, CNN, and Bi-LSTM approaches.

Table 4. Anomaly detection outcomes of EDML-RHADIOTF with other existing models

Models	**mAP (%)**
EDML-RHADIOTF	96.20
YOLOv10	84.36
CNN	84.36
Bi-LSTM	89.23

5. CONCLUSION

In this study, we introduce an edge-driven ML for real-time health anomaly detection in IoT-based healthcare: a modular framework (EDML-RHADIOTF). The EDML-RHADIOTF involves data preprocessing, feature extraction and anomaly classification. In comparison to previous solutions, the suggested EDML-RHADIOTF model shown an outstanding enhancement in anomaly detection based on an analysis of its performance outcomes. With a 96.55% accuracy rate in both reduced and full feature space, SVM performed better across anomaly classification of IoT attacks. A reduction in computing response time, which is necessary for quick response and real-time attack detection, complemented this improvement.

REFERENCES

[1] Goumidi, H. and Pierre, S., 2025. Real-Time Anomaly Detection in IoMT Networks Using Stacking model and a Healthcare-Specific Dataset. *IEEE Access*.

[2] Babbar, H. and Rani, S., 2025. AI-Based Anomaly Detection for Proactive Security Measures in Consumer Healthcare Devices in Internet of Things Network.

[3] Ali, A., Montanaro, T., Sergi, I., Carrisi, S., Galli, D., Distante, C. and Patrono, L., 2025. An Innovative IoT and Edge Intelligence Framework for Monitoring Elderly People Using Anomaly Detection on Data from Non-Wearable Sensors. *Sensors*, *25*(6), p.1735.

[4] Abdulkhudhur, S.M., Abboud, S.M., Najim, A.H., Kadhim, M.N. and Ahmed, A.A., 2025. A Hybrid Deep Belief Cascade-Neuro Fuzzy Approach for Real-Time Health Anomaly Detection in 5G-Enabled IoT Medical Networks. *International Journal of Intelligent Engineering & Systems*, *18*(5).

[5] Alsalman, D., 2024. A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. *IEEE Access*, *12*, pp.14719-14730.

[6] Alharith, R., Ahmed, H., Ibrahim, A.O., Saleh, M.A., Saule, A. and Saltanat, A., 2025, May. Anomaly Detection in IoT Healthcare Security using Machine Learning Methods. In *2025 IEEE 5th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 1-6). IEEE.

[7] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M. and Cao, Z.J., 2020. A practical model based on anomaly detection for protecting medical IoT control services against external attacks. *IEEE Transactions on Industrial Informatics*, *17*(6), pp.4260-4269.

[8] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M. and Cao, Z.J., 2020. A practical model based on anomaly detection for protecting medical IoT control services against external attacks. *IEEE Transactions on Industrial Informatics*, *17*(6), pp.4260-4269.

[9] Parvathi, G.S., Alekya, V., Sridevi, N. and Archana, P., 2024. ML Driven Anomaly Detection for IoT Edge Devices: Insights from ADMM-Based Frequency Management. *International Journal of Communication Networks and Information Security*, *16*(5), pp.600-609.

[10] El Baltaji, G., 2022. *Anomaly Detection at the Edge implementing Machine Learning Techniques* (Doctoral dissertation, Politecnico di Torino).

[11] Raje, V.V., Goel, S., Patil, S.V., Kokate, M.D., Mane, D.A. and Lavate, S., 2023. Realtime Anomaly Detection in Healthcare IoT: A Machine Learning-Driven Security Framework. *Journal of Electrical Systems*, *19*(3).

[12] Khan, M.M. and Alkhathami, M., 2024. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Scientific Reports*, *14*(1), p.5872.

[13] Nawaz, M. and Ahmed, J., 2022. Cloud-based healthcare framework for real-time anomaly detection and classification of 1-D ECG signals. *Plos one*, *17*(12), p.e0279305.

[14] Al Abdulwahid, A., 2022. Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models. *Computational Intelligence and Neuroscience*, *2022*(1), p.2037954

[15] Desai, M., Rumale, A. and Asadinia, M., 2025, May. SHIELD: Securing Healthcare IoT with Efficient Machine Learning Techniques for Anomaly Detection. In *2025 IEEE World AI IoT Congress (AIIoT)* (pp. 0521-0528). IEEE.

[16] Rajaprakash, S., Basha, C.B., Nithya, M., Karthik, K., Aggarwal, N. and Kayathri, S., 2024. RNN-Based Framework for IoT Healthcare Security for Improving Anomaly Detection and System Integrity. *Babylonian Journal of Internet of Things*, *2024*, pp.106-114.

[17] Tawakuli, A., Havers, B., Gulisano, V., Kaiser, D. and Engel, T., 2025. Survey: Time-series data preprocessing: A survey and an empirical analysis. *Journal of Engineering Research*, *13*(2), pp.674-711.

[18] Yaseen, N.A., Hadad, A.A.A. and Taha, M.S., 2021, October. An anomaly detection model using principal component analysis technique for medical wireless sensor networks. In *2021 International Conference on Data Science and Its Applications (ICoDSA)* (pp. 66-71). IEEE.

[19] Tawakuli, A., Havers, B., Gulisano, V., Kaiser, D. and Engel, T., 2025. Survey: Time-series data preprocessing: A survey and an empirical analysis. *Journal of Engineering Research*, *13*(2), pp.674-711.

[20] Hosseinzadeh, M., Rahmani, A.M., Vo, B., Bidaki, M., Masdari, M. and Zangakani, M., 2021. Improving security using SVM-based anomaly detection: issues and challenges. *Soft Computing-A Fusion of Foundations, Methodologies & Applications*, *25*(4).