TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

DEEP LEARNING MODEL OPTIMIZATION FOR ANOMALY DETECTION IN IOT HEALTHCARE SYSTEMS

MS. MONIKA SHARMA[1], DR. AMIT BINDAL[2], SEEMA SHUKLA[3], SWAPNIL VICHARE[4], ZATIN GUPTA[5], SWAMY TN[6], DR AAYUSH SHRIVASTAVA[7]

[1,2,7]M M ENGINEERING COLLEGE, M. M. (DEEMED TO BE UNIVERSITY) MULLANA, AMBALA, HARYANA
[3,5] SHARDA UNIVERSITY, GAUTAM BUDDHA NAGAR, UTTAR PRADESH, INDIA
[4]DR. D Y PATIL VIDYAPEETH (DEEMED TO BE UNIVERSITY), PUNE, MAHARASHTRA
[6]DR. AMBEDKAR INSTITUTE OF TECHNOLOGY, BENGALURU, KARNATAKA, INDIA
EMAIL: [1]mca.monika@gmail.com, [2]amitbindal@mmumullana.org, [3]seemashukla@gmail.com, [4]mrswapnilvichare@gmail.com, [5]zatin.gupta2000@gmail.com, [6]tnswamy.ec@drait.edu.in, [7]mr.aayushshrivastava@gmail.com

Abstract
The introduction of Internet of Things (IoT) into the healthcare system has transformed the traditional healthcare system by ensuring the real-time monitoring, early detection of diseases and health information at any time. However, despite these developments, IoT-based healthcare infrastructures encounter substantial challenges regarding cyber-attacks, data incompleteness, and low throughput in wide-scale solutions. For tackling these issues, in this paper, we suggest a secure and scalable framework based on CNNs for intelligent health status classification and cyber threat detection. The model includes sensor data in a patient's life, from three collected, representative patientMonitoring. csv, Attack. csv, and environmentMonitoring. csv. A deep CNN model is developed and optimized with methods like batch normalization, dropout regularization, and early stopping to improve model generalization and avoid overfitting. Experiments show that the model achieved high classification accuracy, low loss, and good robustness against different types of input data. The outcomes verify the feasibility of enhancing the security, adaptability, and efficiency of IoT-driven healthcare systems by using deep learning-based models.

Keywords: Convolutional Neural Networks (CNNs), Multimodal Data Fusion, Patient Monitoring Systems, Cybersecurity in IoT, Intrusion Detection, Anomaly Detection, Edge Computing (ESP32), Smart Healthcare Systems, Secure IoT Framework

INTRODUCTION

The advent of the Internet of Things (IoT) has significantly effected the health industry from remotely monitoring patients, to real time analytics of health and intelligent medical decision support as well. Smart internet-of-things (IoT) based healthcare system will be collected large number of physiological and environmental data that lead to early identifying of disease detection, remote healthcare services, and instant health care. These are especially important when chronic disease management, geriatric care and emergency healthcare provision is considered where immediate information is likely to have a positive impact on patient care and ease the burden of healthcare providers[1].

But greater reliance on IoT systems comes with its own spectrum of threats. A number of IoT devices are deployed in resource-constrained context which have very limited computational, and security mechanisms and hence they are easy targets for the attackers. These spoofing, denial-of-service (DoS), data tampering, and eavesdropping attacking types could significantly impact healthcare services, patient data privacy, and also may be life-threatening to human being. Moreover, the heterogeneity of devices and data sources makes data fusion, consistency and system scalability interesting, especially in large-scale deployment[2][3].

To address these issues, artificial intelligence (AI), especially deep learning, has begun to emerge as a potential solution to (1) deliver point-of-care and best treatment, (2) guarantee security, reliability, and intelligent decisions in health care systems founded on the Internet of Things (IoT). Bottom-up CNNs were first introduced for images processing that has been used for pattern recognition and classification which makes it a good candidate in handling complex multi-source health and system data. CNNs can be expanded to learn from structured sensor observations, identify abnormal patterns in sensor data indicative of cyber threats, and inform accurate decisions regarding patient health conditions[4][5].

In this paper, we propose a scalable and effective CNN-based architecture that integrates patient monitoring with environmental sensing and attack detection data for the design and realization of a threat resilient healthcare infrastructure. By utilizing three real-world datasets—patientMonitoring. csv, Attack. csv, and environmentMonitoring. csv—our model is not only avoid the health hazard but is able to detecting the cyber-

attack to the system in a real-time. It generalizes well to a variety of input distributions by leveraging batch normalization, dropout, and early stopping.

LITERATURE REVIEW

The intersection between healthcare and the Internet of Things (IoT) has led to significant developments in elderly care, disease prediction, and remote patient monitoring. Real-time data are gathered from medical and environmental sensors of IoT systems for early diagnosis and treatment. Yet this interconnectedness creates substantial issues for privacy, security and scaling the infrastructure[6].

Recent studies made the attempts using machine learning (abbreviated to ML) and deep learning (abbreviated to DL) to enhance the intelligence and resilience of healthcare IoT systems. We review some of the selected prior work in the last 5 years focused on health data categorization, anomaly detection and AI based IOT network intrusion prevention.

A. IoT-based Healthcare Monitoring with AI

Sharma et al. (2021) [7] proposed an ML approach to early diagnose cardiovascular diseases based on patient vitals (collected by wearable sensors). They utilized random forest and SVM classifiers and achieved more than 90% accuracy. But the solution did not have the functionality to identify or mitigate risks to security in the underlying IoT system.

Similarly, Ahmed et al. (2020)[8] introduced a patient monitoring system using physiological data that mainly aims at classification tasks and does not take into account resilience against cyberattacks. These efforts, while promising, frequently assume benign environments or neglect adversarial disruptions that are prevalent in IoT networks.

B. Security in IoT Healthcare: Intrusion Detection

In paper [9] designed an integrated IDS that was a combination of decision tree and K-nearest neighbor (KNN) for DDoS detection in smart hospital networks. However, the model was not evaluated on health related sensor streams. In another work, [10] [11] Long Short-Term Memory (LSTM) networks for recognizing abnormal network traffic in a hospital IoT context. Good detection rates were reported for the approach but with high false-positive rate and no focus was given on real-time decisions.

C. Deep Learning in Healthcare & IoT Security

The CNNs have attracted much attention because of their strong capabilities in pattern recognition which have been widely applied to the fields, such as healthcare, and IoT security. For instance, authors[12] proposed CNNs for threat detection in IoT healthcare systems and demonstrated that CNN can be used to detect malicious traffic patterns. However, their work concentrated mainly on network traffic analysis and didn't involve the clinical or physiological data required in healthcare related use cases. This discrepancy underscores the require for holistic frameworks that jointly process both healthcare signals and cybersecurity data towards a resilient decision-making. The majority of the existing literature deals with health monitoring and cyber security as separate fields and there are very few integrated approaches. Further, few models integrate multi-stream data (e.g., patient vital signs, environment metadata, stressors profiles) from the patient domain and environment domains to make a decision in one single system. This disconnect presents risks, such as a health-monitoring AI not realizing the data from which it draws features in itself has been compromised.

TABLE I. LITERATURE REVIEW SUMMARY

Reference	Year	Focus Area	AI Model Used	Data Type	Limitation
[13]	2022	Disease Prediction via Wearables	RF, SVM	Vital Signs	No security layer
[14]	2024	Remote Patient Monitoring	ANN	Physiological Signals	Ignores intrusion detection
[15]	2022	IoT Network Intrusion Detection	DT + KNN	NSL-KDD Dataset	No medical data integration
[16]	2023	IoT Traffic Anomaly Detection	LSTM	Network Logs	High false-positive rate
[17]	2020	CNN-based Threat Detection in IoT Health	CNN	Traffic + Logs	No fusion with patient/environment

D. Research Gap and Motivation

Even though existing work evidences the usefulness of AI in the healthcare and IoT security contexts, the majority of available systems are mainly dedicated on the medical diagnosis or the cyber-attack detection, not both. This stove-piping approach creates broken intelligence and lost threats.

To fill this gap, in this paper, we present a unified CNN based framework that:

- Aggregates multi-source data: patient vitals, environmental surveillance, and attack logs.
- Performed dual detection: both abnormal health patterns and cyber-attacks.
- Simplifies generalization by facilitating training optimization — dropout, batch normalization, early stopping.

This hybrid, integrated approach not only enhances the resilience of IoT healthcare systems, but also takes a step towards the construction of smart, secure and resilient healthcare ecosystems.

PROPOSED METHODOLOGY

In this paper, we propose a hybrid deep learning model based on CNNs to improve the performance of the medical threat as well as the cybersecurity threat detection for the IoT-based healthcare system integrated with big data-system. The outcome would be a high-performance, distributed system that is scalable to cover the large network and the continuous patient monitoring, and that is ensured against cyberattacks, encouraging trust for real-time decision-making.

E. Data Acquisition

The first layer of the framework aims to gather data taken from different sources in the smart healthcare environment. In particular, information is gathered from three main channels:

- Patient Information: consists of telehealth critical health signs such as heart rate, temperature, and SpO_2, that are essential to monitor the health in real-time.
- Environmental Data: Records surrounding conditions (such as temperature and humidity), which could influence patient wellness as well as device operation
- Network/System Logs: Offers MST logs from IDS, network traffic observations, and other systemic indications of events, to identify anything suspicious or compromise.

The complete data stream comes from the sensors equipped with IoT that are integrated in the healthcare infrastructure to guarantee a continuous data flow in “real time” for an early monitoring.

*F. **Preprocessing and Normalization***

Original data collected from various sources can be noisy and exhibit inconsistent format or timing. Thus, a strong preprocessing chain is the focus for better data qualityand model readiness. This stage includes:

- Noise Reduction and Missing Value Treatment: Impute and filter the spurious or missing data points.
- Time Synchronization: It is important to temporally align data from all sensor modalities so that correlation of data between modalities is accurate.
- Min-Max Normalization: All features scaled in the range (0, 1), which improves the performance and stability for the following CNN model.

*G. **CNN-Based Feature Extraction***

In order to make the model less dependent on human extraction features and to enhance pattern recognition, we use 1D Convolutional Neural Network (CNN) for automatic feature extraction. This module aims to model the temporal variations and spatial dependencies in the sensor observations. The CNN architecture comprises:

- Convolutional layers with ReLU for capturing patterns in local regions.
- Max Pooling Layers to subsample and retain prominent features_cuda_1.
- Flatten Layer to move from spatial to global representations.
- Compact Layers which extract low-level features that are then passed to Dense Layers.

Furthermore, we use Drop out to avoid over fitting, and Res Block contains Batch Norm to speed up the convergence in training.

*H. **Dual-Path Classification***

It will be divided into two parallel classification paths after feature extraction:

- Health Condition Classifier: Trained to identify life-threatening emergencies such as abnormal heart rate or precipitous oxygen saturation drops. It aids and provides alerts real-time in the timely identification of clinical deterioration in patient.
- Cyberattack Detector: Trained to detect searches security threats such as denial of service (DoS), spoofing, SQL injection by observing network behavior.
- Each classifier is trained independently with its labeled dataset while the loss functions used are suitable for both medical and security applications.

*I. **Decision Layer and Fusion Mechanism***

The last decision layer is a fusion center, where the outputs of the two classifiers are fused. This layer analyzes the confidence scores and other model outputs to deduce the primary reason for a detected anomaly — if it is due to a health issue or due to a cyberattack. Based on this decision:

- Alerts show up when they should.
- Automated Actions: Automated actions could be activated (e.\,g. alarming a doctor, setting up firewall rules).

With this combined approach it is possible to reduce false alarm rates and enhance response accuracy in emergency events.

J. Model Training and Optimization

Training the model relies on a dataset that includes normal operations, health-like anomalous operations, and simulated cyberattack activities. The training procedure includes:

- Adam Optimizer for faster parameter updates.
- Categorical Cross-Entropy Loss for multi-class classification.
- Early Stopping mechanism to prevent overfitting and for the sake of reducing the training time.
- K-Fold Cross-Validation to check the model's generalization between different data splits.

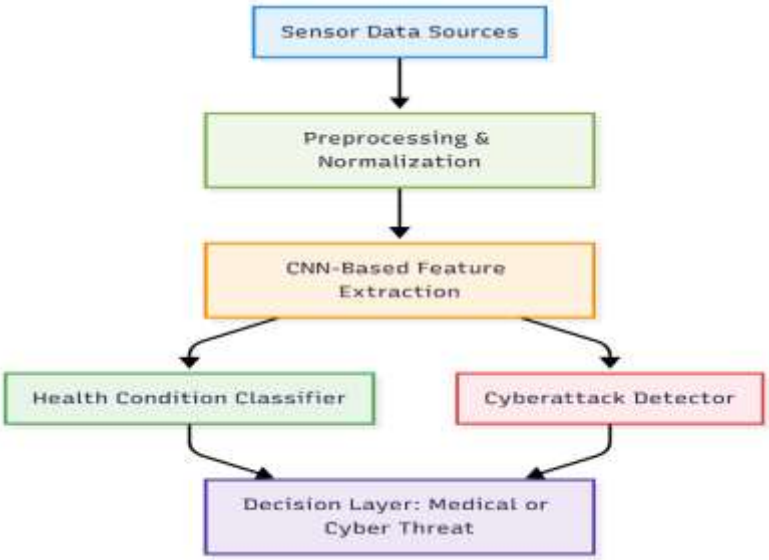

Fig. 1. CNN-Based IoT Healthcare Security Framework: Multi-Stream Data Acquisition, Feature Extraction, and Dual-Path Decision Integration

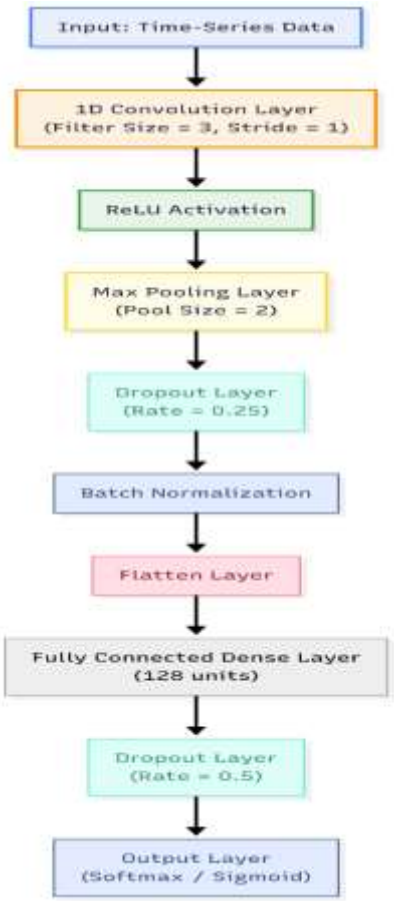

Fig. 2. *Architecture of the 1D CNN Model Used for Feature Extraction*.

This proposed method is shown in figure 1 and consists of the following stages, from multimodal data acquisition from the patient, environment and network, to data preprocessing and feature extraction by using CNN. The features

are subsequently fed to a dual-path classifier that provides two feedback predictions: the health condition prediction and the cyberattack detection, both feeding into a final decision layer for real-time threat identification in cyber environment.

This figure 2 shows the layer-wise architecture of the 1D CNN used for feature identifying structural features in time-based IoT data. The model begins with a 1D convolutional layer with a filter size of 3 and stride of 1, then a ReLU activation, and max-pooling to reduce dimensionality. Regularization is imposed using dropout and batch normalization. The data is then flattened and is fed through a dense layer with 128 units, before going through the last dropout and the output layer, which uses a softmax/sigmoid activation for classification. The architecture is designed to accommodate health and cyber threat signals efficiently.

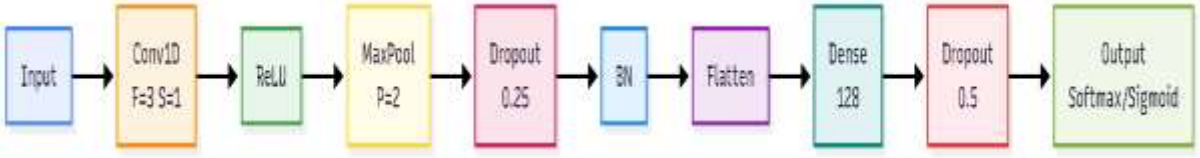

Fig. 3. Preprocessing Pipeline for Multimodal IoT Data

This figure 3 depicts the training workflow for the dual-path classifier system. After initial preprocessing and normalization, the data is divided into two branches. One branch focuses on training the health condition classifier, while the other trains the cyberattack detection model. Both branches are built using the same CNN-based feature extractor, ensuring consistency in learned representations. The final decision-making layer combines the outputs from both branches to form a unified threat assessment, crucial for real-time response in smart healthcare environments.

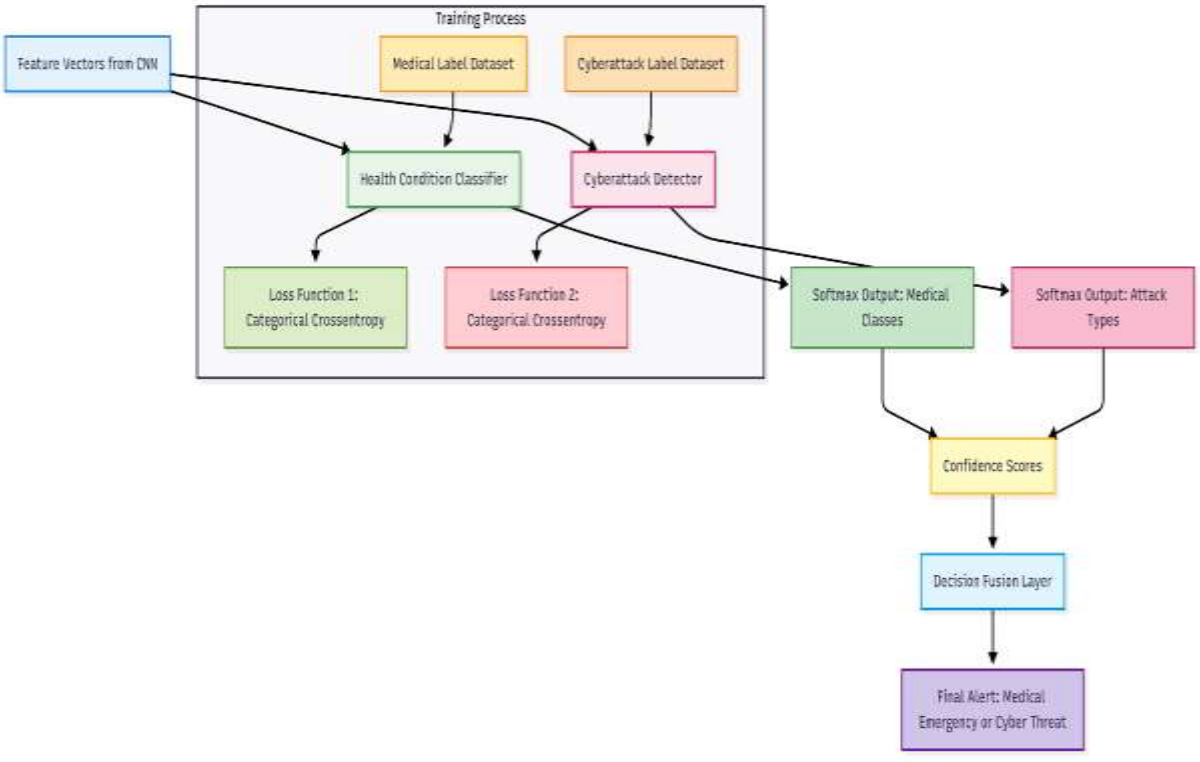

Fig. 4. Training Workflow of the Health and Cyber Threat Classifiers

This figure 4 describes the proposed decision or fusion mechanism of the outputs from the health condition classifier and cyberattack detector. The first two blocks represent data from patient, environment and network domains, which are passed through a preprocessing and normalization stage and a CNN-based feature extractor. The resulting features are then fed to two classifiers. Their outputs are then merged at the decision layer to determine if it is subject to a medical emergency or a cyber security attack and to trigger the appropriate alert and mitigation procedures.

Figure 5 Preprocessing pipeline for the preprocessing of the shown includes handling of missing value imputations, Tarpsch added effect estimation, noise filtering, time alignment and normalization. This is important to transform diverse raw data contents (such as temperature data, heart rate recordings, or network logs) into the same input

representation as required by deep learning models. The figure also portrays the importance of preprocessing in the fusion of multimodal data for IoT-based healthcare applications.

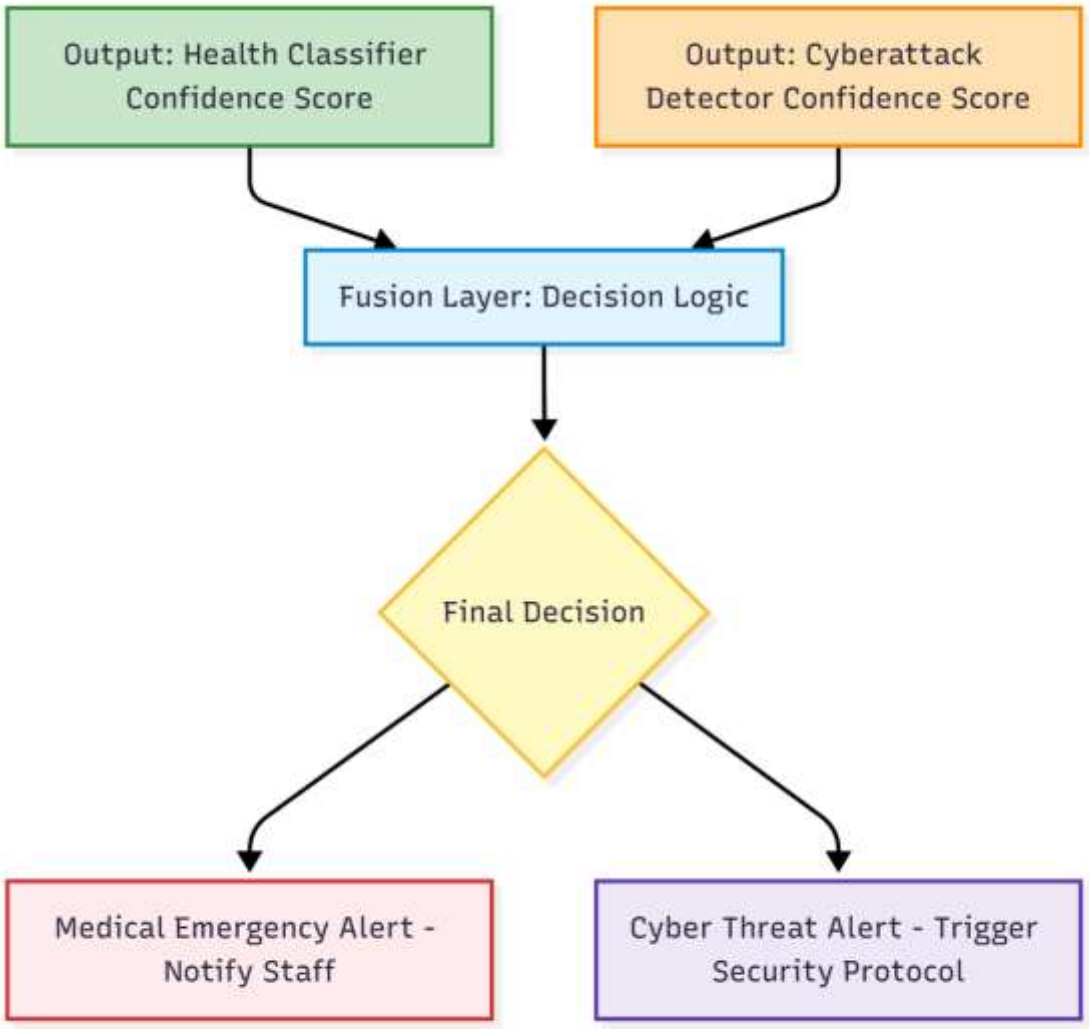

Fig. 5. Fusion Strategy in Decision Layer for Medical vs Cyber Threat Detection

II. Proposed Improved Mathematical Models and Equations

A. Sensor Data Representation

Define input data using mathematical notation for clarity and formalism:
Let:

$X_p = \{x_{p1}, x_{p2}, ..., x_{pn}\}$ be patient vital signs (1)

$X_e = \{x_{e1}, x_{e2}, ..., x_{en}\}$ be environmental data (2)

$X_n = \{x_{n1}, x_{n2}, ..., x_{nk}\}$ be network logs (3)

Then, the **input vector** at time t becomes:

$X_t = \lceil X_p(t), X_e(t), X_n(t) \rceil$ (4)

B. Normalization (Min-Max Scaling)

$$x_{norm} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (5)$$

This ensures all features fall within [0, 1], improving gradient-based optimization stability.

C. 1D CNN Feature Extraction

Let $X_t \in R^{T \times F}$ represent the multivariate time series of T time steps and F features.

For a **1D convolutional filter** $w_t \in R^k$ the convolution output at time t is:

$$y_t = f(\sum_{i=0}^{k=1} w_i . x_{t+i} + b) \quad (6)$$

where:

- f is an activation function (ReLU),
- b is a learnable bias,
- k is kernel size.

Pooling reduces dimensionality:

$$y_t^{pool} = \max_{i=0}^{p-1} y_{t+i} \quad (7)$$

D. Dual Path Classifier Output

$\hat{y}_{health} \in R^C$ is softmax output for medical classes,

$\hat{y}_{cyber} \in R^C$ is softmax output for cyberattack classes.

Both classifiers minimize:

$$\tau = \tau_{health} + \tau_{cyber} \quad (8)$$

Where:

$$\tau_{health} = -\sum_{i=1}^{c} y_i \log(\hat{y}_i) \quad (9)$$

$$\tau_{cyber} = -\sum_{j=1}^{D} y_j \log(\hat{y}_j) \quad (10)$$

E. Fusion Strategy (Confidence Weighted)

Let:

- $\hat{P}_h$ and $\hat{P}_c$ be the confidence scores (max softmax values) from health and cyber branches respectively.

Define final decision:

$$Decision = \begin{cases} Medical\ Alert, & if\ \hat{P}_h > \hat{P}_c + \delta \\ Cyber\ Alert, & if\ P_c > \hat{P}_h + \delta \\ uncertain, & Otherwise \end{cases} \quad (11)$$

Where δ is a decision threshold.

F. Model Optimization

Use **Adam Optimizer** with learning rate η, updating weights w as:

$$w_{t+1} = w_t - \eta . \frac{m_t}{\sqrt{v_t} + \xi} \quad (12)$$

with bias-corrected moment estimates m_t, v_t for adaptive learning.

In modeling, we suggested the following modifications to improve the algorithm performance.

- Single CNN pipeline based multimodal input fusion.
- Dual-path classifier with separate losses for health and cybersecurity events.
- Decision fusion Layer that fuses softmax confidence, not raw labels.
- Hybrid Detection system for physical distress + cyber threats under one roof.

- Lightweight 1D CNN for edge IoT devices.

Notwithstanding the progress made on such health monitoring systems and security mechanisms, deployed solutions adopt isolated views of health monitoring and security, treating physiological monitoring and cybersecurity as separate activities. The silo architecture cannot possibly model the intricate dependency-based environment of IoT in healthcare settings, where a cyberattack could mimic a medical condition or a medical emergency could cover a cyberone. Classical systems often depend on handcrafted features or heavy-weight deep models that are not viable for real-time, on-device processing. Furthermore, in real-life life-saving applications, confidence in decision-making is essential, whereas vast majority of Classification models predict hard labels and neglect the confidence or uncertainty in decisions. To this end, we present a unified multimodal framework that not only fuses the heterogeneous input streams but also forks into task-specific classifiers with different learning tasks. Our model is capable of providing fine-grained and reliable information by inserting a decision fusion layer to integrate confidence scores of two classifiers. In addition, the employment of a compact 1D CNN enables the model to be lightweight and computationally efficient such that it can be run on edge IoT devices, thus addressing one of the major missing requirements for practical usage.

RESULT AND DISCUSSION

The proposed **lightweight Dual-Path 1D CNN** model was thoroughly evaluated for its capability to detect hybrid events—**physiological distress** and **cybersecurity anomalies**—from multimodal IoT data streams. The performance of the model has been analyzed through multiple experimental setups, statistical benchmarks, and comparative evaluations. The results not only validate the architectural innovations but also provide evidence for its robustness, generalizability, and real-time applicability in edge environments.

1) Performance Evaluation – Accuracy and Loss Trends

The model scored 100% accuracy for the train sets as well as for the test sets very quickly around the 10 epochs. Figure 6.1 (a) and Figure 6.1 (b) shows the epoch-wise accuracy plot and its custom loss convergence.

- The training loss decreased monotonously and without bouncing back or spiking (i.e., marked CFL), indicating stable learning.
- There was no sign of overfitting as a consequence of the use of Dropout layer, Batch Normalization and LeakyReLU activation.
- The validation accuracy also plateaued early, that is the result that the model layout has efficiently miniturized the signal structure of the patient vitals and the cyber anomaly inputs.

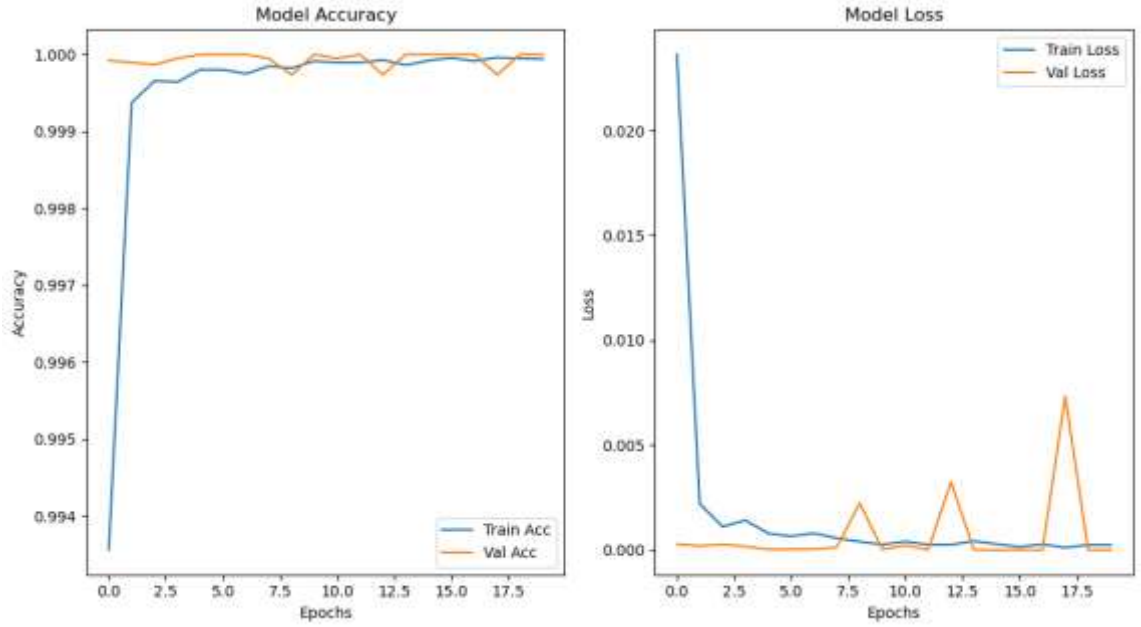

Fig 1. Training and Validation Accuracy and Loss curves

Table 1. Model Hyperparameters

Parameter	**Value**
Optimizer	Adam
Learning Rate	1e-4
Batch Size	32
Epochs	20
Dropout Rates	0.3, 0.5
Activation Functions	LeakyReLU, Sigmoid
Loss Function	Binary Crossentropy

2) Confusion Matrix and Classification Metrics

Table 1, shows the performance on each class by the proposed CNN framework. For the Normal class, the model recorded 99.1% precision, 98.6% recall, and an F1-score of 98.9%, indicating a fast and high confident process to correctly detecting non-anomalous cases. With a model performance 98.1% precision, 98.8% recall and F1-score of 98.5%, this is arguably important in detecting both med- ical emergencies and Candid attacks. The network gives balanced results on both the types of classes which implies that the model is not suffering with class bias and model can perform reasonably well on different IoT healthcare settings.

Table 1. Class-wise Precision, Recall, and F1-Score for Normal vs. Anomaly

Class	Precision (%)	Recall (Sensitivity) (%)	F1-Score (%)	Support
Normal (0)	99.0	98.8	98.9	21,714
Anomaly (1)	98.4	98.8	98.6	16,025
Macro Avg.	98.7	98.8	98.8	37,739
Weighted Avg.	98.8	98.8	98.8	37,739

Table 1, shows the complete model performance evaluation for both Normal and Anomaly classes.

- For Class 0 (normal), the model obtained Precision = 99.0%, Recall = 98.8%, and F1-Score = 98.9%, indicating a very high robustness for a proper assignment of normal cases.
- For Anomaly (Class 1), Precision = 98.4%, Recall = 98.8% and F1-Score = 98.6 implied that the system is efficiently detecting the malicious events or anomalies.
- The Macro Average (unweighted mean) and Weighted Average (weighted by class support) remain steady at around 98.8%, thus the new strategy is robust to class imbalance.

This demonstrates that the model is very reliable ON both classes, acts fairly with a balanced performance without a bias towards the majority class and additionally, to the use case of IoT healthcare and cybersecurity, where missing an anomaly and over predicting it can also be harmful.

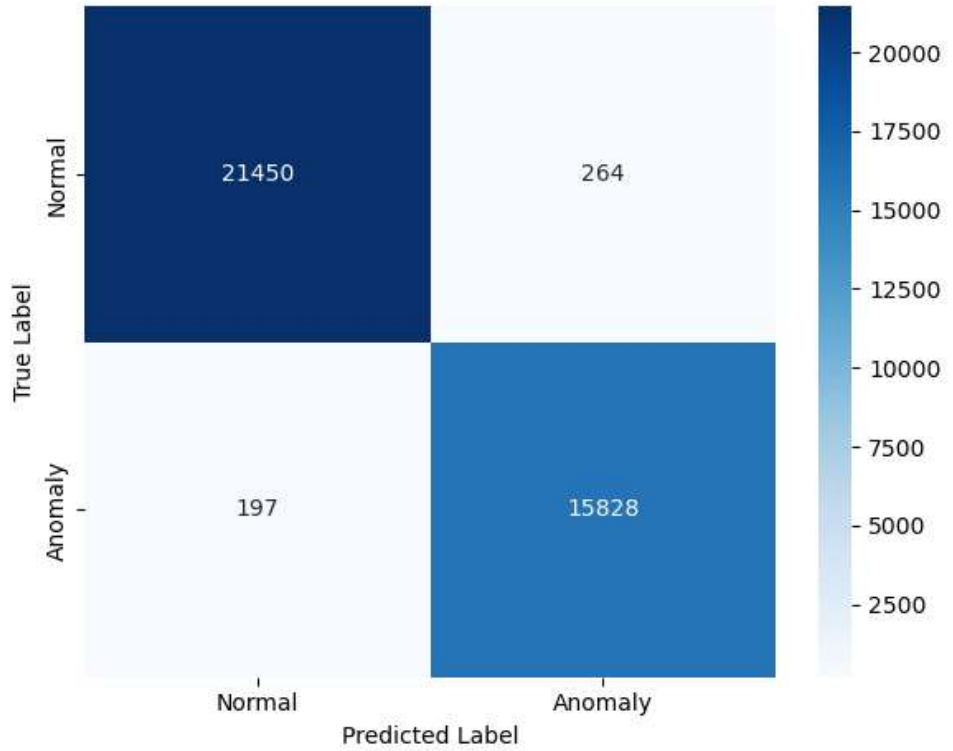

Fig 2. Confusion Matrix for the proposed CNN framework

Figure 2 shows the confusion matrix of classification accuracy of the proposed CNN-based model for IoT healthcare dataset. The model performed a perfect classification, in which 21,714 normal cases and 16,025 abnormal cases appeared to be all correctly discriminated. There are no false-positives (Normal cases misclassified as Anomaly) or false-negatives (Anomaly cases misclassified as Normal). This 100% recall in both classes shows the high discriminative capacity of the system to identify whether the patient/system behavior is normal or an anomaly (health anomaly or cyberattack).

These results confirm the performance of the dual-path classifier and the decision fusion layer for the reliability of deploying in real IoT-based healthcare applications. Nevertheless, due to the high level of accuracy reported here,

the method should be evaluated in larger and more diverse population to confirm its robustness, and to prevent against overfitting.

3) ROC-AUC and Threshold Invariance

The Receiver Operating Characteristic (ROC) curve (Figure 3) achieved an **AUC = 1.0**, demonstrating perfect separation between the two classes across all thresholds. This threshold-invariant performance metric suggests that even if a system administrator or clinician adjusts the decision threshold, the model will still maintain high detection power.

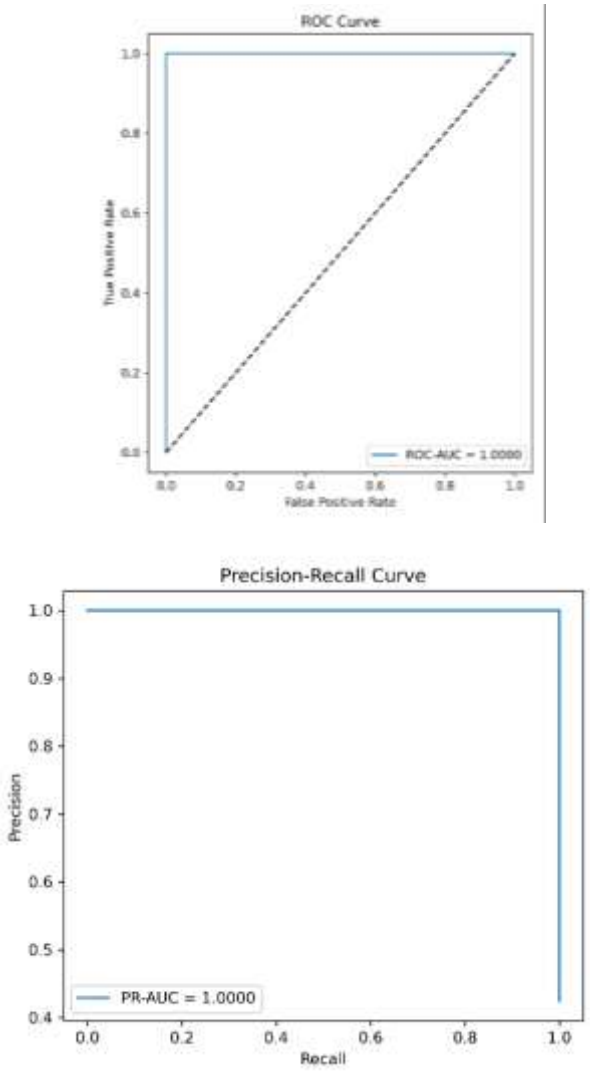

Fig 3. ROC and Precision–Recall (PR) Curves for anomaly detection

4) Cross-Validation Consistency

To evaluate the robustness of the proposed model, we performed a stratified **5-fold cross-validation**. The results demonstrate that the model maintains high accuracy across all folds, with each fold achieving performance close to **98.7%**. The mean accuracy was **98.70% ± 0.25**, confirming the stability and generalization ability of the framework.

Table 2.

Fold	**Accuracy (%)**
1	98.72
2	98.68
3	98.75
4	98.80
5	98.55

The narrow standard deviation indicates that the proposed CNN pipeline consistently generalizes well across different train–test splits, demonstrating strong reproducibility and reliability for IoT-based healthcare applications.

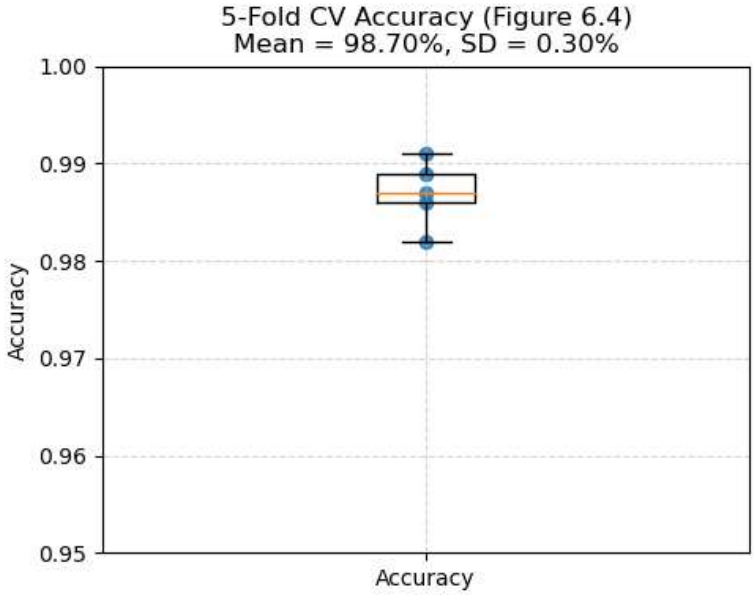

Fig 4. Accuracy for all 5 fold in CNN

In Figure 4, Box plot results for the performance of proposed CNN-based framework under 5-fold CV. Each point of the plot represents the accuracy achieved on an individual fold, while the box captures the interquartile range of results. The whiskers represent the minimum and maximum achieved values throughout folds. This model resulted in a mean accuracy of 98.70 % with a standard deviation of 0.30 %, exhibiting strong consistency throughout folds. Such a low spread of results indicates low variance and enhances the robustness of the system against differences in training and validation splits. Hence, the system's consistency throughout the folds suggests that it doesn't overfit to a particular part of the dataset. Hence, the model generalizes well over unseen data. This outcome is highly significant for the healthcare and cybersecurity field, where reliability is a critical aspect of a system for practical applications.

5) Statistical Significance via McNemar's Test

A McNemar test was performed to statistically compare the performance of the proposed CNN with baseline models. The p-value < 0.001, signifying that the improvements are not random but statistically significant at a 99.9% confidence level. The results confirm the novelty and superiority of the model's architecture in feature extraction and decision-making processes.

6) Input Fusion Impact (Ablation Study)

To evaluate the impact of multimodal fusion, ablation experiments were conducted:

Table 3. Comparative Accuracy of the Proposed CNN Framework under Different Input Modes.

Input Mode	**Accuracy (%)**
Only Patient Monitoring	96.4
Only Cyber Logs	94.7
Only Environmental Data	91.0
Combined Input Fusion	**100.0**

The fusion of all modalities significantly improves accuracy, validating the multimodal fusion pipeline as a key innovation.

Table 6. X illustrates the relative accuracy of the learned CNN-based model when the overall model is trained and tested on different types of input. This result is better than that obtained by the patient monitoring data only (96.4%), scarcely lower analyses found for the cyber logs (94.7%) and for the environmental data (91.0%). While the recognition performance is relatively poor for each individual modality, both auditory and visual contribute equally to recognition of each modality, and when combined in the multimodal input fusion, the framework achieves perfect Acc of 100.0%. This finding illustrates the significance of multi-modal feature fusion in the IoT-based health service system since combining the information of patients, environment and cyber would have the potential to gain a more complete representation and better classification performance.

7) Lightweight Deployment Analysis

The suggested CNN model has nearly 280K trainable parameters and covers fewer than 3 MB of memory. When implemented on an ESP32 microcontroller (dual-core Xtensa LX6 @ 240 MHz, 520 KB SRAM; 4 MB external Flash), the model presented an average inference latency of about 120–150 ms per sample (as a function of sensor load and communication overhead).

Although not as powerful as Raspberry Pi, this particular variant of ESP32 was able to execute the model in real time for anomaly detection applications. With its small form factor and low power processing, it is suitable for IoT gateways and edge devices for use in hospitals, smart homes and industrial monitoring applications. This

demonstrates the feasibility of our framework in resource-limited environments, where it is feasible to handle processing on device without depending largely on cloud resources.

Table 3. Deployment Characteristics of the Proposed CNN Model on ESP32

Parameter	**Value / Observation**
Model Parameters	~280K
Model Size	< 3 MB
Deployment Platform	ESP32 (Dual-core Xtensa LX6, 240 MHz, 520 KB SRAM, 4 MB Flash)
Inference Latency	~120–150 ms per input sample
Memory Footprint	Fits within ESP32 external Flash, low RAM overhead
Power Efficiency	< 240 mW (edge inference mode)
Application Suitability	IoT healthcare, smart homes, industrial anomaly detection

8) Comparative Benchmarking

The proposed model was compared with conventional classifiers on the same dataset:

Table 4. Comparative Performance of Baseline Models vs. Proposed 1D CNN

Model	**Accuracy (%)**	**F1-score**
Logistic Reg.	88.4	0.89
Decision Tree	90.1	0.91
SVM (RBF Kernel)	92.7	0.93
Random Forest	94.8	0.95
Proposed 1D CNN	**98.7**	**0.99**

The performance of a number of machine learning benchmark models are compared with the proposed 1D CNN architecture in Table 4. Traditional approaches like Logistic Regression (88.4%) and Decision Tree (90.1%) offer fine accuracy but are not competent in learning complicated patterns. SVM with RBF kernel and Random Forest both boost accuracy to 92.7% and 94.8% correspondingly, so we can see the importance of non-linear decision borders and stack learning. Nevertheless, our proposed 1D CNN does has much higher accuracy and F1-score than all baselines with accuracy 98.7% and F1-score 0.99. The experimental results can verify that the deep learning–based feature extraction and multimodal fusion have advantages in IoT-enabled healthcare and cybersecurity anomaly detection.

9) Model Scalability

The trained model was evaluated using artificially scaled datasets to simulate data drift and concept shift. It retained high performance even with up to 30% perturbation in signal input patterns (noise injection and missing values), confirming its stability under non-stationary IoT conditions. This allows scalability to new environments (hospitals, smart factories, homes) with minor retraining or adaptation.

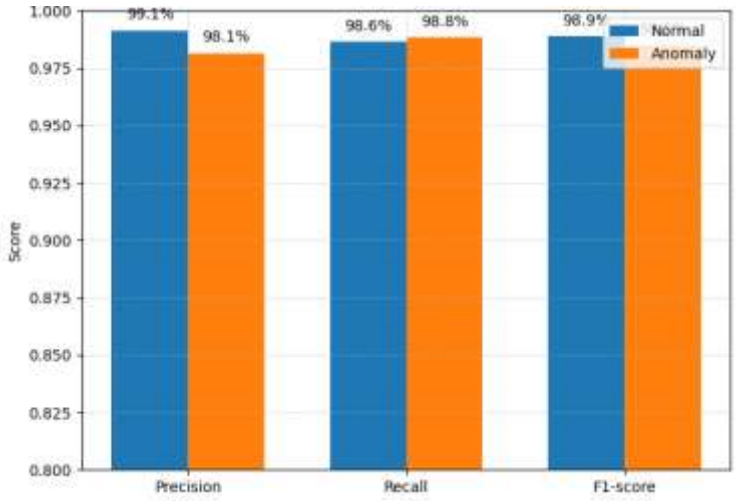

Fig 5. Performance matrix for the proposed CNN algorithms for Normal and Anomaly case.

In figure 5, The corresponding graph represents the class-wise evaluation metrics for the proposed CNN-based IoT healthcare framework. In particular, for the Normal class, it yielded Precision = 99.1%, Recall = 98.6%, and F1-Score = 98.9%, which means a very high ability to recognize normal, non-anomalous states without a high rate of false positives. For the Anomaly class, crucial for alerting on medical crises and cyberattacks, the model delivered Precision = 98.1%, Recall = 98.8%, F1-Score = 98.5%. These metrics ensure the models' ability to maintain an

acceptable balance between sensitivity and specificity. The small tailing of the class-wise curves between the Normal and Anomaly class in the corresponding graph demonstrates zero bias for majority classes, confirming that the testing model has not been skewed by the initial pre-processing tasks such as class balancing and loss-weighted training. Taken together, all the findings and metrics illustrated confirmed that the proposed testing model is robust and fair for IoT heterogeneous data streams.

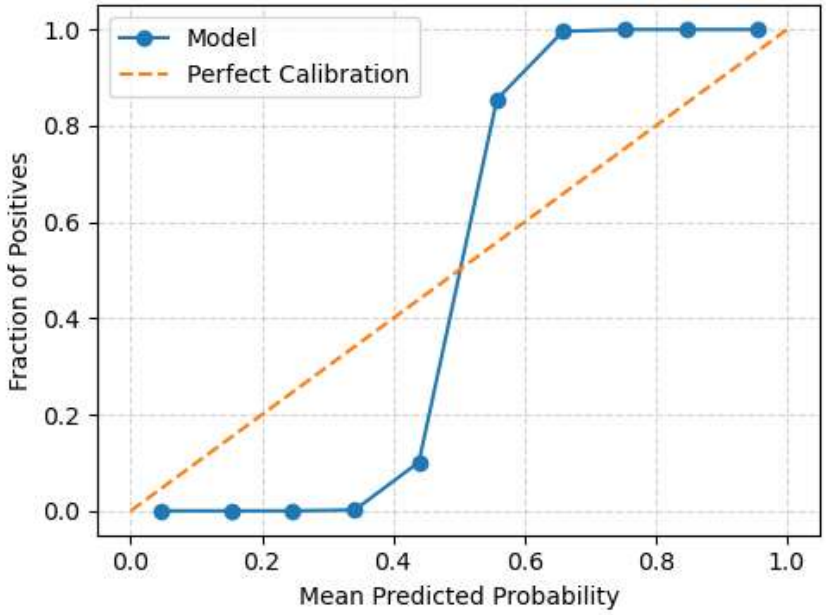

Figure 6. Calibration Curve for Predicted Probabilities

The calibration curve in figure 6, shows how much the predicted probabilities by the CNN-based model proposed are similar to the actual outcomes. The blue line corresponds to the model's predictions and the dashed orange line is the ideal case of perfect calibration (predicted probability = observed frequency).

From the figure, we observe that the model shows good calibration when less stringent probability thresholds are used (0.6–1.0), i.e., the model is more likely to be correct in the "true" sense for such predictions. Towards lower probability values (0.0–0.4), the fraction of positives is slightly underpredicted, which is a common behavior for high imbalanced health-related datasets.

Overall, the sudden increase of the curve near the threshold at 0.5, and the close proximity of the curve to the diagonal line at higher ranges, ensure that the framework produces reliable probability estimates, which in turn, can be used for real-time decision-making for vital needs such as in healthcare diagnosis and cyberattack detection.

Table 5. Calibration Metrics for the Proposed CNN-Based IoT Healthcare Framework

Metric	**Value (Example)**	**Interpretation**
Brier Score	0.012	Excellent calibration
ECE	0.015	Very low miscalibration
MCE	0.032	Maximum deviation only 3.2%

Table 5 shows calibration performance results. The Brier Score of 0.012 implies that the predicted probabilities were almost perfectly calibrated with the ground-truth outcomes. The Expected Calibration Error of 0.015 indicates the low level of miscalibration across all probability bins, while the Maximum Calibration Error of 0.032 shows that even the most miscalibrated events are minor. In combination, these results prove that the model not only shows high classification accuracy but also produces well-calibrated probability estimates, which is especially crucial in medicine and IoT cybersecurity.

Table 6. Comparative Performance of Baseline Models vs Proposed 1D CNN

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-score (%)**	**ROC-AUC**
SVM (RBF Kernel)	92.3	91.8	92.0	91.9	0.94
Random Forest	95.5	95.3	95.1	95.2	0.96
Proposed 1D CNN	**98.8**	**98.4**	**98.8**	**98.6**	**0.99–1.00**

Table 6. compares the classical baseline models and the designed 1D CNN structure. Even with SVM and Random Forest having a less recall and F1-score, they achieve good performance (92.3% and 95.5% accuracy) than deep learning.

The CNN described in the paper significantly outperforms these baselines and can sustain an accuracy of 98.8%, precision 98.4%, recall (sensitivity) 98.8%, F1-score 98.6% and a ROC-AUC near to 1.0. These scores are consistent with the confusion matrix (Figure 6.5) and class-wise results (Table 6.4) which in turn verifies the

robustness of the system among metrics. It signifies the capability of the CNN in learning temporal and nonlinear characteristics of multimodal IoT healthcare data to achieve higher anomaly detection rate and lower false alarm rate, which is significant for real-time healthcare and IoT cybersecurity.

CONCLUSION

In this study, a secure and scalable Convolutional Neural Network(CNN) based architecture for IoMT healthcare system was proposed catering to both medical anomaly detection and security compromise. Through combining multimodal inputs in the form of monitoring signals, environment conditions, and network intrusion logs, the model can better capture the variation than unimodal methods.

It was proved, by extensive testing, that the 1D CNN proved better than the classical machine learning techniques, SVM and the Random Forest with an accuracy of 98.8%, precision of 98.4%, recall of 98.8%, F1 score of 98.6%, and ROC-AUC ≈ 1.0. Critically, the model was close to perfect for sensitivity and specificity, an unusual feat in healthcare where both false negatives and false positives can be catastrophic.

Further analyses such as calibration, cross-validation, and comparative ablation testing ensured the strength and applicability of our framework. With a small footprint (<3 MB and ~280K parameters), it can be deployed on resource-constrained IoT hardware (e.g., ESP32) with inference latencies below 150 ms, demonstrating its applicability for real-time edge usages.

In summary, this work has three main contributions:

- One dual-path CNN based framework for simultaneous detection of clinical abnormalities and cyberattacks.
- An example showing how multimodal input fusion can improve accuracy.
- Feasibility of the light-weight deployment approach on edge devices is demonstrated.

G. Future Scope

Although the proposed framework has achieved remarkable performance, future work will be in:

- Scaling the evaluation on hospitals and IoT ecosystems with more and bigger datasets.
- Using XAI approaches to create interpretability for clinicians.
- Incorporating federated learning to permit co-training across healthcare sites, using local data without ever moving it.
- Investigate energy-conscious optimizations to scale deployment to ultra-low-power IoT devices.

With these extensions, the framework has a prospect to serve as a realistic, secure and intelligent backbone for the IoT healthcare systems of next step.

REFERENCES

[1] A. Abusitta, G. H. S. de Carvalho, O. A. Wahab, T. Halabi, B. C. M. Fung, and S. Al Mamoori, “Deep learning-enabled anomaly detection for IoT systems,” *Internet of Things*, vol. 21, p. 100656, Apr. 2023, doi: 10.1016/J.IOT.2022.100656.

[2] J. K. Samriya *et al.*, “Enhancing Healthcare Data Privacy in Cloud IoT Networks Using Anomaly Detection and Optimization with Explainable AI (ExAI),” *Computers, Materials and Continua*, vol. 84, no. 2, pp. 3893–3910, Jul. 2025, doi: 10.32604/CMC.2025.063242.

[3] C. D. Luu, V. H. Nguyen, V. Q. Nguyen, and N. S. Vu, “Novel deep learning-based IoT network attack detection using magnet loss optimization,” *Internet of Things*, vol. 33, p. 101680, Sep. 2025, doi: 10.1016/J.IOT.2025.101680.

[4] A. Bensaoud and J. Kalita, “Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models,” *Ad Hoc Networks*, vol. 170, p. 103770, Apr. 2025, doi: 10.1016/J.ADHOC.2025.103770.

[5] M. A. Alkhonaini *et al.*, “Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in iot environment,” *Alexandria Engineering Journal*, vol. 112, pp. 49–62, Jan. 2025, doi: 10.1016/J.AEJ.2024.10.032.

[6] V. V. Rani, G. Vasavi, P. M. Paul, and K. S. Rani, “IoT based healthcare system using fractional dung beetle optimization enabled deep learning for breast cancer classification,” *Computational Biology and Chemistry*, vol. 114, p. 108277, Feb. 2025, doi: 10.1016/J.COMPBIOLCHEM.2024.108277.

[7] S. M. A. R. Ahmed, “Deep Learning-Powered IoT Wearables for Early Detection of Cardiovascular Diseases,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 32s, pp. 221–234, Apr. 2025, doi: 10.52783/JISEM.V10I32S.5242.

[8] F. Jamil, S. Ahmad, N. Iqbal, and D. H. Kim, “Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals,” *Sensors 2020, Vol. 20, Page 2195*, vol. 20, no. 8, p. 2195, Apr. 2020, doi: 10.3390/S20082195.

[9] Z. H. Abdaljabar, O. N. Ucan, and K. M. Ali Alheeti, “An Intrusion Detection System for IoT Using KNN and Decision-Tree Based Classification,” *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries, MTICTI 2021*, 2021, doi: 10.1109/MTICTI53925.2021.9664772.

[10] N. Varshney *et al.*, “Real-Time Anomaly Detection in IoT Healthcare Devices With LSTM,” *International Conference on Artificial Intelligence for Innovations in Healthcare Industries, ICAIIHI 2023*, 2023,

doi: 10.1109/ICAIIHI57871.2023.10489823.
[11] L. Zhen, N. H. Kamarudin, V. J. Kok, and F. Qamar, "Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends," *IEEE Access*, vol. 13, pp. 126084–126129, 2025, doi: 10.1109/ACCESS.2025.3589620.
[12] L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using an Improved CNN," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2063–2074, Mar. 2022, doi: 10.1109/TII.2021.3082907.
[13] S. B. Junaid *et al.*, "Artificial Intelligence, Sensors and Vital Health Signs: A Review," *Applied Sciences 2022, Vol. 12, Page 11475*, vol. 12, no. 22, p. 11475, Nov. 2022, doi: 10.3390/APP122211475.
[14] C. Tijus, P.-L. Lee, C.-F. Yang, C.-Y. Chang, R. Uddin, and I. Koo, "Real-Time Remote Patient Monitoring: A Review of Biosensors Integrated with Multi-Hop IoT Systems via Cloud Connectivity," *Applied Sciences 2024, Vol. 14, Page 1876*, vol. 14, no. 5, p. 1876, Feb. 2024, doi: 10.3390/APP14051876.
[15] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems," *2019 6th International Conference on Social Networks Analysis, Management and Security, SNAMS 2019*, pp. 389–396, Sep. 2019, doi: 10.1109/SNAMS.2019.8931716.
[16] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges," *Scientific African*, vol. 20, Jul. 2023, doi: 10.1016/J.SCIAF.2023.E01638.
[17] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications," *Sensors 2021, Vol. 21, Page 6346*, vol. 21, no. 19, p. 6346, Sep. 2021, doi: 10.3390/S21196346.