Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 8 (2026) 3230

Journal of the Nigerian Society of Physical Sciences

Dynamic-kernel CNN-LSTM for real-time intrusion detection in low-power healthcare IoT systems

Osita Miracle Nwakeze[a,*], Naveed Uddin Mohammed[b], Obaze Caleb Akachukwu[c], Umerah Anthony Tochukwu[d], Oji Nkechi Blessing[d], Ibeh Sylvarine Chinasa[a], Odeh Christopher[c]

[a]*Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria*
[b]*Department of Computer Science, Lindsey Wilson University, Columbia, Kentucky, USA*
[c]*Department of Computer Science, Dennis Osadebay University, Asaba, Delta State, Nigeria*
[d]*Department of Computer Engineering, Federal University of Technology, Owerri, Imo State, Nigeria*

Abstract

Cybersecurity has become a serious concern in healthcare Internet of Things (IoT) systems, where connected medical devices support patient monitoring, diagnosis, and treatment but remain vulnerable to attacks. This paper presents a Dynamic-kernel Convolutional Neural Network–Long Short-Term Memory (DyK-CNN-LSTM) architecture for energy-efficient intrusion detection in healthcare IoT environments. The model combines SoftMax-gated dynamic convolutional kernels with bidirectional LSTM layers to learn multi-scale spatial dependencies and temporal correlations in network traffic. Causal pooling is incorporated to support low-latency, simulation-based real-time inference on low-power devices. Experiments on the IoT Healthcare Security and CICIoMT-2024 datasets produced an integrated-dataset accuracy of 98.42%, precision of 98.35%, recall of 98.41%, F1-score of 98.38%, and false alarm rate of 1.58%. Attack-specific analysis showed consistently strong detection across DDoS, replay, ransomware, brute-force, data-exfiltration, botnet, scanning, and backdoor attacks. Hardware-aware simulation on a 100 MHz ARM Cortex–M4 target indicated an energy consumption of 92.3 μJ and a latency of 24.5 ms per inference, with real hardware validation planned as future work. The proposed DyK-CNN-LSTM framework therefore offers a balanced design for accurate, scalable, and energy-aware intrusion detection in medical IoT systems.

DOI:10.46481/jnsps.2026.3230

Keywords: Healthcare IoT, Intrusion detection system, Dynamic-kernel CNN, Bidirectional LSTM, Causal pooling

Article History :
Received: 28 November 2025
Received in revised form: 20 March 2026
Accepted for publication: 31 March 2026
Available online: 03 June 2026

Communicated by: B. J. Falaye

1. Introduction

The development of healthcare Internet of Things (IoT) devices, including implantable pacemakers, continuous glucose monitors (CGMs), and insulin pumps, has improved patient monitoring and chronic disease management by enabling continuous physiological data collection and remote diagnosis [1, 2]. These devices are commonly used in ambulatory and home-care environments and often require long operating periods on small, sealed batteries. For example, modern CGMs are reported to support multi-day operation, whereas leadless pacemakers operate within limited battery capacities and strict power budgets. These design constraints mean that many med-

*Corresponding author Tel. No.: +234-802-207-0309.
Email address: ma.nwakeze@coou.edu.ng (Osita Miracle Nwakeze)

ical IoT devices cannot support heavyweight software stacks or frequent firmware updates without affecting device lifetime or patient care [3].

Conventional intrusion detection models, particularly those based on deep neural networks such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, can provide high detection accuracy in network environments. However, they are often computationally expensive and energy intensive when deployed on edge devices [4]. Implementing full-size CNN/LSTM pipelines on resource-constrained microcontrollers can increase the power consumed per inference and reduce battery life by orders of magnitude. This trade-off has motivated growing TinyML and low-power inference research for microcontrollers with sub-megabyte flash and RAM footprints [5]. Recent work on the quantified on-device energy requirements of naive deep models further indicates that such models can require several orders of magnitude more energy than well-designed TinyML alternatives, reinforcing the need for architectures designed specifically for ultra-low-power devices [6].

Current IoT intrusion detection systems (IDSs) often rely on fixed convolutional kernels, which are limited in their ability to respond to the bursty and non-stationary nature of IoT network traffic. In such environments, attacks such as short DDoS bursts, slow stealthy exfiltration, and replay bursts against Bluetooth Low Energy links vary in temporal scale and intensity [7]. Input-adaptive convolution methods, also called dynamic or adaptive convolution, learn to adjust kernel weights according to the input. These methods have been proposed in related areas to improve flexibility without substantial increases in model cost and provide a promising direction for energy-aware IDS design, where receptive fields learn to respond to traffic variations rather than applying a single fixed kernel size [8].

Intrusion detection in IoT and healthcare IoT contexts has been widely studied, with particular attention given to hybrid deep learning models that combine spatial feature extraction and temporal sequence modelling. Early approaches used CNNs to identify local traffic dynamics and LSTMs to identify sequential behaviour. For example, a CNN–LSTM hybrid was proposed to improve threat detection on the N-BaIoT, IoT-23, and CICIDS2017 datasets. That framework integrated principal component analysis (PCA), model quantization, and pruning to optimize performance in resource-constrained settings, achieving accuracies of up to 99% [9]. Similarly, CST-AFNet used multi-scale CNNs, bidirectional gated recurrent units (BiGRUs), and dual attention to focus on important temporal and channel features, showing near-perfect performance on the Edge-IIoTset dataset [10].

To improve detection efficiency and reduce false positives, several studies have incorporated attention mechanisms and feature selection methods. Hybrid frameworks integrating CNNs, LSTMs, and attention layers have been evaluated on UNSW-NB15 and CICIDS2017 datasets, achieving accuracy rates above 97% [11, 12]. Other works have focused on network-level robustness by combining deep architectures with optimization models, such as Adam, and SHAP-based feature analysis, achieving near-perfect precision and recall under adversarial settings [13, 14].

Lightweight optimization and adaptive learning have also been introduced for resource-constrained IoT and Industrial IoT (IIoT) systems. Attention-enhanced CNN–LSTM models using particle swarm optimization (PSO) dynamically learned significant features while maintaining computational efficiency [15]. Self-attention-based CNN models (SA-DCNN) addressed class imbalance and redundant features, with strong results on IoTID20 and Edge-IIoTset datasets [16]. Multi-branch architectures combining CNN, LSTM, and gated recurrent unit (GRU) layers improved feature-learning granularity and achieved 100% binary classification accuracy on TON_IoT datasets [17]. Hybrid autoencoder–LSTM models in healthcare-specific IoT systems have detected anomalies in Internet of Medical Things (IoMT) network traffic and imbalanced datasets with high AUC scores [18]. Explainable AI approaches, such as XIoT, have emphasized interpretability in high-speed network environments while maintaining accuracies above 99% on multiple benchmarks [19]. Attention-based CNN IDS systems, such as ABCNN-IDS, have improved focus on low-instance features and shown robustness on IoTID20, Edge-IIoTset, ToN_IoT, and CIC-IDS2017 datasets [20].

Finally, ensemble and hybrid models combining XGBoost, CNN, LSTM, and transformer designs have placed greater emphasis on high detection accuracy, energy efficiency, and scalability. These frameworks have outperformed conventional single-model approaches, achieving accuracies above 98%, reduced computational latency, and low energy consumption, which are critical for battery-constrained IoT devices [21–25]. A recent attention-trained one-dimensional Conv-BiLSTM architecture has also performed well in real IoT traffic settings, with an AUC–ROC score of 0.995, and is suitable for capturing both spatial and temporal associations [26].

Taken together, the studies reviewed show the effectiveness of hybrid deep learning frameworks for IoT intrusion detection. Table 1 summarizes selected existing literature with respect to datasets and reported accuracies.

Although numerous hybrid CNN–LSTM models [9–17] have shown high detection accuracy on general IoT and IIoT datasets, most have been evaluated on resource-rich platforms and do not adequately address the ultra-low-power constraints of battery-limited healthcare IoT devices. Moreover, existing adaptive convolution approaches, such as that of Ref. [7], improve flexibility in general vision tasks but have not been tailored to the bursty, multi-scale, and protocol-heterogeneous nature of medical IoT traffic. In this context, the proposed DyK-CNN-LSTM model makes the following contributions:

1. an input-adaptive dynamic kernel gating mechanism that uses a SoftMax-weighted combination of kernel sizes $\{3, 5, 7\}$ to capture short bursts such as DDoS and longer-term patterns such as ransomware with minimal parameter overhead;
2. integration of a bidirectional LSTM with causal pooling to enable low-latency, memory-efficient real-time inference without buffering full sequences;

3. a cross-dataset harmonization and joint-training strategy using IoMT-specific flows from the IoT Healthcare Security and CICIoMT-2024 datasets to support robust generalization across single- and multi-protocol environments; and
4. reporting of accuracy, F1-score, false alarm performance, energy consumption, and latency in comparison with baseline IDS models across the evaluated datasets.

These elements provide a targeted balance of detection performance and deployability in energy-constrained medical settings, as evaluated through hardware-aware simulations.

The remainder of this paper is organized as follows. Section 2 presents the proposed methodology. Section 3 discusses the experimental results and analysis. Section 4 concludes the paper and outlines directions for future work.

2. Methodology

This section describes the architecture and deployment workflow of the proposed Dynamic-kernel CNN–LSTM (DyK-CNN-LSTM) framework for real-time intrusion detection in healthcare IoT systems operating under battery constraints. It covers the system architecture, dataset acquisition, preprocessing, model design, and evaluation metrics. The study focuses on securing IoMT networks found in modern healthcare environments, including intensive care units, emergency wards, ambulatory monitoring systems, and home-based patient monitoring setups. These environments rely on low-power devices, including ECG monitors, CGMs, infusion pumps, and smart insulin systems, that continuously transmit physiological data. Because such devices have constrained computing power and battery life, an intrusion detection model suitable for embedded deployment is essential.

2.1. System architecture

The DyK-CNN-LSTM is designed around the power and memory limitations of battery-constrained healthcare IoT devices, such as devices with approximately 0.3 mAh batteries and less than 1 MB RAM, including those present in CGMs and insulin infusion pumps. Although direct on-device deployment on implantable systems is not considered in this work, the simulation results suggest possible feasibility under such restrictions. The proposed architecture addresses these constraints by integrating dynamic spatial feature extraction, temporal sequence modelling, and low-latency real-time decision-making. As shown in Figure 1, the architecture consists of three main components.

2.1.1. Dynamic-kernel CNN

The DyK-CNN module derives spatial patterns from sequential network-traffic features. Unlike classical CNNs, whose kernel size is fixed, DyK-CNN uses a collection of kernels $\{3, 5, 7\}$ to capture traffic characteristics at different temporal scales:

- short kernels ($k = 3$), which identify rapidly occurring temporary anomalies such as DDoS bursts or traffic spikes;
- medium kernels ($k = 5$), which capture moderately evolving attack patterns; and
- long kernels ($k = 7$), which model persistent trends such as ransomware encryption or slow data exfiltration.

A dynamic gating mechanism assigns adaptive weights to each kernel according to the temporal burstiness of the input flow. This allows the CNN to focus on the most important spatial characteristics of the input in real time.

2.1.2. Bidirectional long short-term memory

The bidirectional LSTM (Bi-LSTM) module learns the temporal dynamics of sequential network flows. By processing sequences in forward and backward directions, Bi-LSTM models can detect long-range correlations and recurring cyberattack patterns. This two-way strategy supports the detection of attacks that evolve gradually over time, such as multi-step intrusions or covert ransomware activity. The Bi-LSTM receives the spatial features extracted by the DyK-CNN module and converts them into temporal representations, which are then processed by the output layer for classification.

2.1.3. Causal pooling layer

The causal pooling layer uses only the final timestep of the LSTM output sequence to make predictions, thereby supporting low-latency real-time inference. Unlike other pooling or sequence aggregation techniques that require the entire sequence, causal pooling reduces memory use and computational time, making the architecture more suitable for resource-constrained medical IoT devices. This design also enables security decisions to be made as new traffic arrives, avoiding buffering delays during always-on monitoring.

2.2. Datasets

To support robust and generalizable evaluation, the proposed DyK-CNN-LSTM model was trained and validated on two complementary public datasets.

2.2.1. IoT Healthcare Security Dataset

The IoT Healthcare Security Dataset [27], which is publicly available on Kaggle, was used to evaluate the proposed DyK-CNN-LSTM framework. It contains 47,071 labelled network flows from diverse healthcare IoT devices, including ECG monitors, CGMs, insulin pumps, and blood pressure monitors. Each flow is characterized by 46 features, including temporal, statistical, and protocol-based attributes such as duration, inter-arrival time (IAT), packet size, and TCP/UDP flags. The flows are labelled as normal or as one of eight attack types, including replay, DDoS, ransomware, and brute-force attacks, representing a realistic combination of malicious and benign traffic patterns.

Table 1: Comparative analysis of techniques and datasets.

Ref.	Technique	Dataset(s) used	Reported accuracy (%)
[9]	CNN + LSTM; PCA + quantization + pruning for device optimization	IoT-23, N-BaIoT, CICIDS2017	IoT-23: 95; N-BaIoT: 99; CICIDS2017: 99
[10]	Multi-scale CNN + BiGRU + dual attention (channel and temporal)	Edge-IIoTset (2.2 million instances)	99.97 (multiclass); 100 (binary)
[11]	CNN + LSTM + attention; PCA + recursive feature elimination	UNSW-NB15	97.89
[12]	CNN + LSTM	CICIoT2023; tested on CICIDS2017	98.42 (CICIoT2023); 97.45 (CICIDS2017)
[13]	Deep CNN (64 convolutional layers) + 16 LSTM layers	CICIDS2017	99.82
[14]	LSTM + CNN; SHAP feature analysis; adversarial evaluation	BoT-IoT	99.87
[15]	CNN + LSTM + attention; PSO for feature selection	Standard IoT intrusion dataset (WIoTSN)	CNN: 98.73; LSTM: 99.87; CNN–LSTM: 99.12; proposed: 98.88
[16]	Self-attention + deep CNN; two-step deduplication cleaning	IoTID20, Edge-IIoTset	IoTID20: 96.89; Edge-IIoTset: 99.95
[17]	Parallel CNN, LSTM, and GRU fusion; SMOTE and median imputation	TON_IoT, CICIDS2017	TON_IoT: 100 (binary); CICIDS2017: 99.49
[18]	Autoencoder (three layers) + LSTM for temporal anomaly detection	CICIoMT-2024 (40 devices, 18 attacks)	94.1

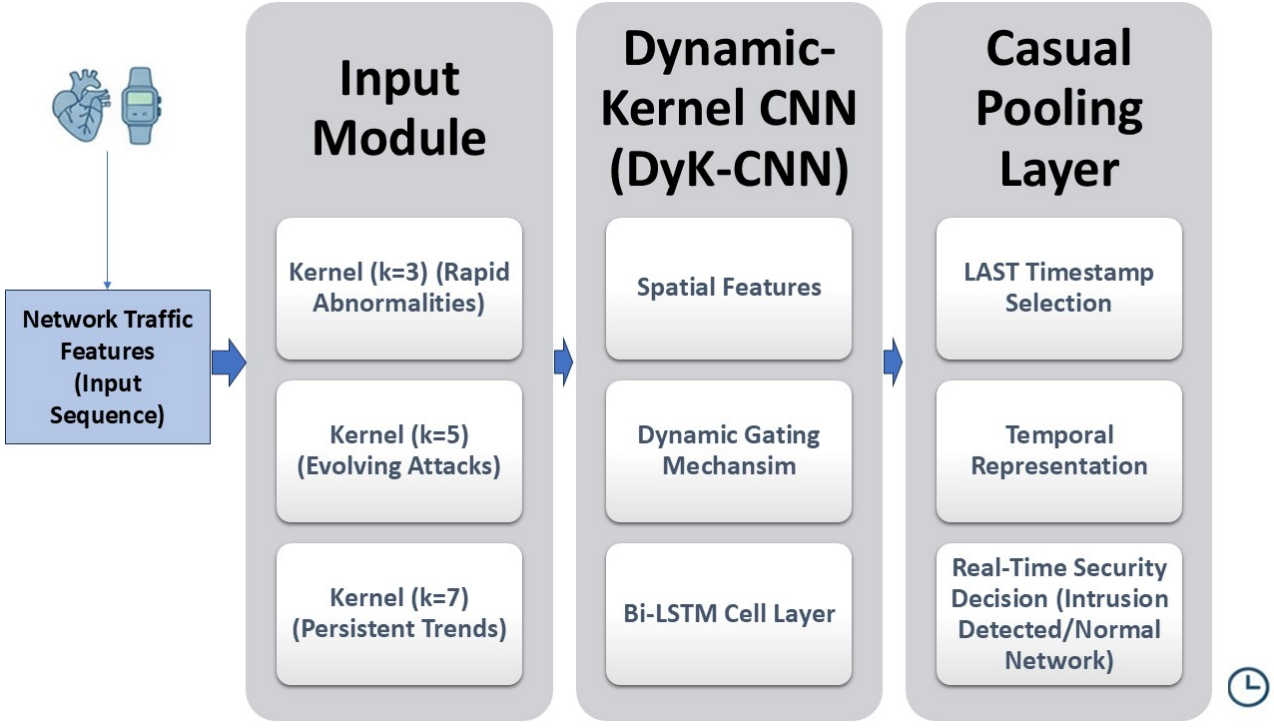

Figure 1: DyK-CNN-LSTM system architecture for healthcare IoT security.

Table 2: Detailed architecture specification of DyK-CNN-LSTM.

Component	Layer/details	Parameters/notes
Input	Shape: (batch, 60 timesteps, 46 features)	–
DyK-CNN	Three parallel Conv1D branches: kernel sizes 3, 5, and 7; 64 filters each; causal padding; ReLU activation	Gating mechanism: dense layer → SoftMax over branches
Bi-LSTM	One bidirectional LSTM layer; 128 hidden units per direction; return_sequences = True; dropout = 0.2; tanh activation	–
Causal pooling	Lambda layer: select last timestep ([:, −1, :])	Enables real-time inference
Classifier	Dense(128, ReLU) → Dropout(0.2) → Dense(num_classes, softmax)	num_classes = attack types + normal
Optimizer	Adam (initial learning rate = 0.001, ReduceLROnPlateau)	Loss: categorical cross-entropy
Total parameters	≈450,000	Approximate

2.2.2. *CICIoMT-2024 Dataset*

To strengthen the generalizability and real-world applicability of the findings, the CICIoMT-2024 dataset [28] from the Canadian Institute for Cybersecurity was integrated. This dataset is substantially larger and more diverse, containing more than 1.2 million network flows generated from 40 physical and simulated IoMT devices communicating across multiple protocols, including Wi-Fi, Bluetooth, ZigBee, and MQTT. It includes 18 detailed attack classes, such as DoS/DDoS, MQTT publish floods, reconnaissance, spoofing, and protocol-specific exploits, providing a comprehensive benchmark for evaluating IDS robustness in heterogeneous medical environments.

2.3. Data preprocessing

A unified data preprocessing pipeline was applied to both the IoT Healthcare Security and CICIoMT-2024 datasets to ensure consistency, compatibility, and robust model training. The pipeline began with feature harmonization, in which common network-flow attributes, such as packet counts, IAT, and protocol flags, were aligned across the two datasets to create a joint feature space. Feature scaling using Z-score standardization was then applied to normalize features to a mean of zero and a standard deviation of one, reducing disparities in feature magnitude and improving convergence during training [29]. Missing values and outliers were addressed using median imputation and clipping to ensure that spurious readings did not dominate the learning process. Protocol and flag features were categorically encoded using one-hot encoding, converting nominal variables into numerical representations suitable for deep learning pipelines. In modern IoT IDS research, standardization has been shown to provide consistent improvements in classifier performance across datasets.

To capture the time-varying nature of IoT traffic, a fixed-length sliding window of $T = 60$ timesteps was used to create a three-dimensional tensor. Such segmentation is compatible with CNN–LSTM hybrids because it allows the models to learn both spatial features and temporal dependencies [30]. The dataset was then split into training (80%) and testing (20%) subsets using stratified sampling to preserve the distribution of attack types and normal flows. Minority-class oversampling was applied where necessary to reduce class imbalance.

2.3.1. Dataset harmonization and label alignment

The two datasets differ in scale, protocols, and attack granularity. To create a joint feature space, the following steps were applied:

- shared features were retained, including flow duration, IAT, packet sizes (mean, forward, and backward), TCP/UDP flags, and protocol type (one-hot encoded);
- dataset-specific features, such as CICIoMT-2024 protocol-specific MQTT fields not present in the Kaggle dataset, were removed or ignored;
- CICIoMT-2024's 18 attack classes were grouped and aligned to the eight common categories in the IoT Healthcare Security Dataset (for example, DoS → DDoS, MQTT floods → DDoS variant, and reconnaissance → scanning), while normal and benign flows were unified as "Normal"; and
- class imbalance was addressed using stratified sampling and minority oversampling through an SMOTE variant during training splits.

This harmonization minimizes distortion while enabling cross-dataset generalization, although some protocol-specific nuances may introduce minor bias, which was mitigated through joint training.

2.4. Model design

The framework proposed in this study integrates a dynamic-kernel convolutional network with a bidirectional LSTM to capture both spatial and temporal patterns in healthcare IoT traffic. The architecture is optimized for low-latency and energy-constrained implementation, enabling real-time intrusion detection on battery-limited healthcare devices. The complete layer configuration and hyperparameters are provided in Table 2.

2.4.1. Dynamic-kernel CNN

For an input sequence $X \in \mathbb{R}^{B\times T\times F}$, where B is the batch size, T is the sequence length, and F is the number of features, the dynamic convolution at layer l is defined in equation (1) as [7]:

$$\mathrm{Out}_l = \sum_{k\in\{3,5,7\}} \alpha_{l,k} \cdot \mathrm{Conv}_k(X), \qquad \alpha_l = \mathrm{softmax}(\theta_l). \quad (1)$$

Here, $\alpha_{l,k}$ represents the learned weight for each kernel size k, allowing the network to adapt to short-term spikes, such as DDoS bursts, and longer-term trends, such as ransomware propagation, in network flows. By dynamically weighting multiple kernel sizes $\{3, 5, 7\}$, DyK-CNN efficiently extracts spatial features while maintaining low computational overhead.

2.4.2. Bi-LSTM with causal pooling

The spatial features extracted by DyK-CNN are passed to a Bi-LSTM to model temporal dependencies using equation (2) [31]:

$$h_t = \text{Bi-LSTM}(x_{\text{cnn}}, h_{t-1}), \qquad \widehat{y} = \mathrm{FC}(h_T). \quad (2)$$

Causal pooling ensures that only the last timestep, h_T, contributes to the prediction $\widehat{y}$, thereby eliminating the need to buffer entire sequences and enabling real-time inference. This combination of DyK-CNN and Bi-LSTM ensures that both bursty anomalies and longer-term traffic patterns are captured for accurate intrusion detection.

2.4.3. Energy and latency estimation

Energy consumption per inference is estimated based on multiply-accumulate (MAC) operations using equation (3) [32]:

$$E = \mathrm{MACs} \times 0.9\,\mathrm{pJ/MAC} \quad (45\,\mathrm{nm}). \quad (3)$$

The latency of the system was evaluated through simulation at 100 MHz. The energy- and latency-aware design considered in this study supports feasibility assessment for battery-constrained devices such as pacemakers, CGMs, and insulin pumps.

2.4.4. Pseudocode for model components

The dynamic kernel gating and overall forward pass are summarized in Algorithm 2.4.4.

Algorithm 2.4.4: Pseudocode for the DyK-CNN forward pass.

```
def dynamic_kernel_gating(x):
  # x:  input tensor (batch, timesteps, features)
  conv3 = Conv1D(filters=64, kernel_size=3,
      padding='causal', activation='relu')(x)
  conv5 = Conv1D(filters=64, kernel_size=5,
      padding='causal', activation='relu')(x)
  conv7 = Conv1D(filters=64, kernel_size=7,
      padding='causal', activation='relu')(x)
  concatenated = Concatenate(axis=-1)(
      [GlobalAveragePooling1D()(conv3),
       GlobalAveragePooling1D()(conv5),
       GlobalAveragePooling1D()(conv7)])
  attn_scores = Dense(3, activation=None)(concatenated)
  weights = Softmax()(attn_scores)
  weighted_output = conv3*weights[:,:,0:1]
      + conv5*weights[:,:,1:2]
      + conv7*weights[:,:,2:3]
  return weighted_output
spatial_features = dynamic_kernel_gating(input_sequence)
temporal = Bidirectional(LSTM(128,
return_sequences=True))(spatial_features)
pooled = temporal[:, -1, :]
output = Dense(num_classes, activation='softmax')(pooled)
```

2.5. Model training and implementation

The proposed DyK-CNN-LSTM architecture was first trained on each dataset separately and then on a combined dataset to evaluate cross-dataset generalization. Combined training ensured that the model learned from both single-protocol traffic distributions in the Kaggle dataset and multi-protocol traffic distributions in the CICIoMT-2024 dataset, enabling a more robust feature representation. Hyperparameters, including learning rate, batch size, dynamic kernel weights, and LSTM hidden units, were tuned using joint validation splits from both datasets.

The intrusion detection framework was implemented in Python 3.10 using TensorFlow 2.12 and Keras as the primary deep learning libraries. The Adam optimizer was used with a learning rate of 0.001 and categorical cross-entropy loss. Stratified sampling was used to create the 80:20 training and testing split while preserving class balance. Training was conducted for up to 50 epochs with a batch size of 64, and early stopping and learning-rate scheduling were applied to improve convergence.

To evaluate deployability, the trained model was converted to TensorFlow Lite Micro format and compiled into a C array using the ARM GNU toolchain for the Cortex–M4 CPU. The resulting model was implemented in the QEMU cycle-accurate ARM emulator to estimate inference latency under simulated embedded conditions. Energy consumption was estimated using McPAT, configured for a 100 MHz target and 45 nm process technology, and the memory footprint was obtained during compilation. This software-only validation assessed whether the proposed model remained within the energy, latency, and memory requirements for efficient healthcare IoT implementation.

3. Results and discussion

The IoT Healthcare Dataset was used to evaluate the proposed framework in terms of its ability to identify and classify different types of cyberattacks targeting IoT-based medical devices. The evaluation metrics were accuracy, precision, recall, F1-score, and false alarm rate (FAR).

Table 3: Performance results of the model.

Metric	IoT Healthcare Security Dataset (%)	CICIoMT-2024 Dataset (%)
Accuracy	98.76	97.88
Precision	98.51	97.35
Recall	98.62	97.48
F1-score	98.56	97.41
False alarm rate (FAR)	1.24	2.12

Table 4: Performance on the integrated IoMT dataset.

Metric	Value (%)
Accuracy	98.42
Precision	98.35
Recall	98.41
F1-score	98.38
False alarm rate (FAR)	1.58

3.1. Multi-dataset model performance

Table 3 presents the performance of the DyK-CNN-LSTM model when trained and tested on the individual datasets. On the IoT Healthcare Security Dataset, the model achieved an overall accuracy of 98.76%, precision of 98.51%, recall of 98.62%, and F1-score of 98.56%. The FAR was 1.24%, reflecting the model's ability to minimize false positives in practical applications. When evaluated on the more complex CICIoMT-2024 dataset, which includes multi-protocol traffic and a wider variety of attacks, the model maintained a robust accuracy of 97.88% and an F1-score of 97.41%.

The performance results in Table 3 show that the proposed model is effective for identifying cybersecurity threats in healthcare IoT systems. The high precision and recall across both datasets indicate a strong ability to identify true threats with few false positives or missed detections. The balanced F1-score further highlights the model's robustness for continuous monitoring in clinical environments, where false alarms and missed attacks can have serious consequences.

3.2. Performance on the integrated dataset

To simulate a real-world deployment scenario involving a diverse ecosystem of medical devices, the IoT Healthcare Security Dataset and the CICIoMT-2024 dataset were merged into a unified dataset. The performance of the proposed model on this integrated dataset is summarized in Table 4. The model achieved an overall accuracy of 98.42% and an F1-score of 98.38%, with a low FAR of 1.58%.

This high performance on the integrated data is a significant result because it demonstrates that the proposed architecture can learn a unified and generalized representation of network intrusion that is robust to the inherent heterogeneity of large-scale IoMT systems.

3.3. Attack-specific detection

To further assess the strength of the model against a broad spectrum of cyberattacks, the test subset of the IoT Healthcare Security Dataset was analysed in terms of attack-specific

Table 5: Performance of the model across attack classes.

Attack type	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Normal	99.10	99.15	98.90	99.02
DDoS	99.45	99.60	99.25	99.42
Replay	99.30	99.18	99.35	99.26
Ransomware	97.75	97.40	98.10	97.75
Brute-force	97.95	98.00	97.85	97.92
Data exfiltration	98.25	98.10	98.45	98.27
Botnet	98.80	98.60	98.95	98.77
Scanning	98.45	98.40	98.50	98.45
Backdoor	98.65	98.50	98.75	98.62

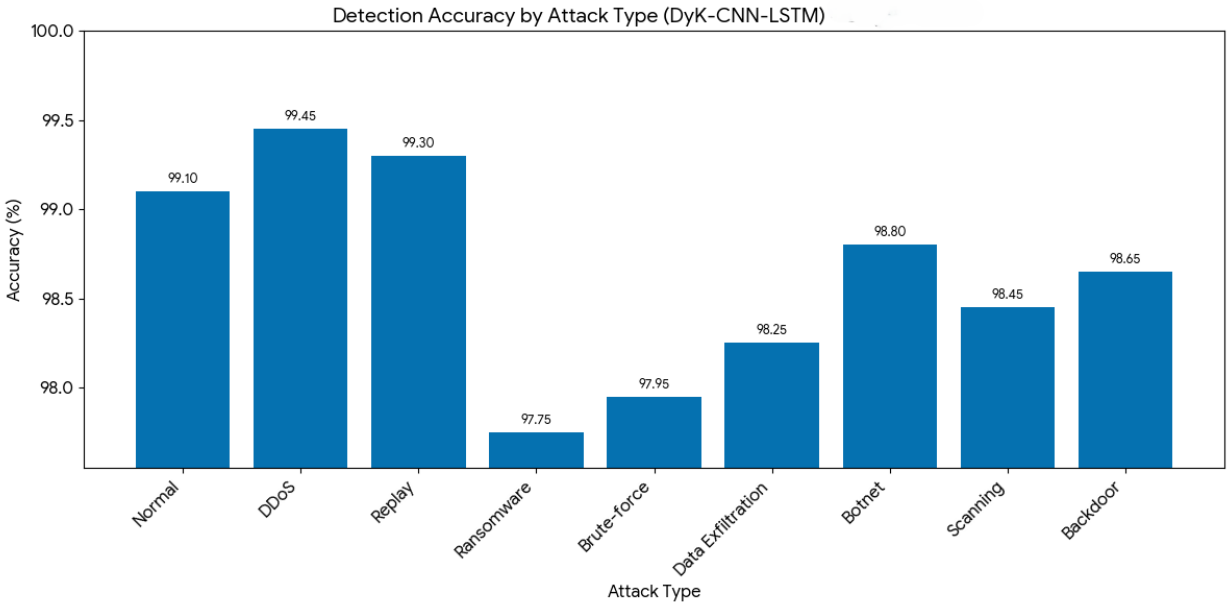

Figure 2: Detection accuracy results of the proposed model across attack classes.

Table 6: Fair comparison with baselines on the integrated dataset.

Model	Accuracy (%)	F1-score (%)	Inference latency (ms)	Energy (µJ)
CNN–LSTM (static)	97.12	96.89	27.3	105.6
Attention CNN–LSTM	97.85	97.62	29.8	118.4
Proposed DyK-CNN-LSTM	98.42	98.38	24.5	92.3

performance. Table 5 summarizes the accuracy, precision, recall, and F1-score obtained for each attack type. The results in Figure 2 show that the model can differentiate successfully between the classes of malicious behaviour commonly observed in healthcare IoT networks.

The model achieved consistently high accuracy across all attack categories, as shown in Figure 2, with F1-scores exceeding 97% in every case. The highest detection performance was observed for DDoS (99.42%) and replay (99.26%) attacks. Detection of ransomware (97.75%) and brute-force (97.92%) attacks was slightly lower than that of the other categories. This reduction can be explained by feature overlap between benign

and malicious traffic at the packet level, because both may have similar connection duration and payload size. The Bi-LSTM component was important for modelling sequential dependencies across flow windows, improving the model's ability to detect slow and stealthy attacks such as data exfiltration (98.27%) and backdoor intrusions (98.62%). Overall, these findings indicate that the framework provides attack-type robustness and can generalize to a broad range of threat behaviours.

3.4. Energy and latency analysis

Energy and latency performance are critical parameters for evaluating the practicality of deep learning models in real-world healthcare IoT systems, because medical devices often operate with limited power and computing capacity. The energy consumption and inference latency of the model were simulated under IoT-device conditions and evaluated at a processor frequency of 100 MHz. The results showed an average energy consumption of 92.3 μJ per inference, indicating the model's lightweight computational footprint. This outcome is supported by the hybrid model's efficient use of convolutional layers for feature extraction and LSTM units for temporal learning, together with dynamic kernel allocation and selective activation during inference.

The average latency of 24.5 ms also indicates that the model can operate within the requirements of many real-time healthcare monitoring applications. This latency is acceptable for most monitoring applications, although further optimization would be required for sub-millisecond control loops. The architecture enables security decisions to be made as new traffic arrives, supporting always-on monitoring with minimal buffering.

3.5. Comparative analysis

To provide a fair evaluation, this study compared the proposed DyK-CNN-LSTM against two baseline models implemented and evaluated under identical preprocessing, dataset split, and simulation conditions on the integrated dataset. These models were:

- Baseline 1: a standard CNN–LSTM model composed of static kernels (kernel size = 5, 64 filters) and a unidirectional LSTM (128 units); and
- Baseline 2: an attention-based CNN–LSTM model [11] composed of a static kernel and additive attention.

All models were trained on the integrated IoMT dataset with the same training parameters. The results of the comparative analysis are reported in Table 6.

The main strengths of the proposed model are its adaptive spatial feature extraction and balanced temporal modelling. As shown in Table 6, the DyK-CNN-LSTM achieved an accuracy of 98.42% and an F1-score of 98.38% on the integrated IoMT dataset, outperforming both the standard CNN–LSTM baseline (97.12% accuracy, 96.89% F1-score) and the attention-based CNN–LSTM baseline (97.85% accuracy, 97.62% F1-score). Unlike static kernel designs, which use a constant receptive field, the dynamic mechanism can extract multi-resolution spatial information effectively, enabling the model to respond to both burst attacks such as DDoS and longer-term trends such as ransomware without adding substantial parameters.

Furthermore, the Bi-LSTM component with causal pooling allows the model to capture forward and backward temporal dependencies while supporting real-time decision-making. Table 6 confirms the efficiency of this design: the proposed model achieved an inference latency of 24.5 ms and an energy consumption of 92.3 μJ per inference, outperforming the standard CNN–LSTM baseline (27.3 ms, 105.6 μJ) and the attention-based baseline (29.8 ms, 118.4 μJ). The hardware-aware simulations show that the model provides a favourable trade-off between detection accuracy and efficiency. Despite its compactness, with approximately 450,000 parameters, the model achieved high detection performance with a low FAR of 1.58%, placing it within the upper tier of intrusion detection models while maintaining the lowest energy and latency among the compared architectures.

These results show that the proposed DyK-CNN-LSTM offers competitive detection performance and clear operational-efficiency improvements over baselines evaluated in the same environment. This trade-off is particularly useful for real-time clinical monitoring systems, where reliability and responsiveness are critical. In addition, the model's SoftMax-based dynamic kernel selection provides a leaner structure than complex ensemble networks. This simplicity may support future interpretability and auditing, which are increasingly important in medical cybersecurity and regulatory compliance.

4. Conclusion

This paper developed and implemented a DyK-CNN-LSTM architecture for smart intrusion detection in healthcare IoT settings. The model combines dynamic-kernel convolutional layers and bidirectional LSTM units to represent multi-scale spatial and temporal dependencies in network traffic data. By integrating two complementary datasets, the IoT Healthcare Security Dataset and the CICIoMT-2024 dataset, the proposed model benefited from a richer and more diverse representation of real-world medical traffic patterns, attack behaviours, and device characteristics. Experimental results demonstrated competitive performance, with an accuracy of 98.42%, precision of 98.35%, recall of 98.41%, F1-score of 98.38%, and a low FAR of 1.58%. Simulation results further indicate practical feasibility, with an average energy consumption of 92.3 μJ and inference latency of 24.5 ms per prediction. These findings support the model's potential for accurate, energy-aware, and real-time medical IoT security.

The success of the proposed model can be attributed to architectural innovations that prioritize both resource efficiency and deployability. Unlike traditional deep or ensemble architectures that require substantial computation and memory, the proposed framework provides competitive detection performance with a compact and energy-conscious design. Its performance across different attack types, including high-volume DDoS as well as stealthy ransomware and exfiltration attacks, indicates

strong generalization. The simpler model structure may also facilitate future interpretability analysis and integration with healthcare cybersecurity monitoring systems.

4.1. Future work

Several research directions are suggested to further improve the applicability of the proposed model:

1. Hardware validation: perform real-device deployment and benchmarking on representative medical-grade hardware, including ARM Cortex–M4 boards and Raspberry Pi platforms, to obtain actual performance and power profiles beyond simulation.
2. Federated learning and edge–cloud collaboration: introduce federated learning frameworks to improve data privacy while maintaining distributed intelligence across medical devices.
3. Explainable AI: incorporate explainable AI methods to provide deeper insight into model decisions and support auditability and clinical trust.
4. Robustness to zero-day and adversarial attacks: extend the dataset with multi-hospital or cross-domain traffic and evaluate resilience to emerging zero-day and adversarial attacks.

These extensions would support the development of next-generation secure, interpretable, and self-adaptive intrusion detection systems for healthcare IoT ecosystems.

Data availability

The datasets used in this study are publicly available at https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset and http://cicresearch.ca/IOTDataset/CICIoMT2024/.

Funding

The authors received no external funding for this study.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

References

[1] S. K. Garg, M. Kipnes, K. Castorino, T. S. Bailey, H. K. Akturk, J. B. Welsh, M. P. Christiansen, A. K. Balo, S. A. Brown, J. L. Reid & S. E. Beck, "Accuracy and safety of Dexcom G7 continuous glucose monitoring in adults with diabetes", Diabetes Technology & Therapeutics **24** (2022) 373. https://doi.org/10.1089/dia.2022.0011.

[2] T. Martens, R. W. Beck, R. Bailey, K. J. Ruedy, P. Calhoun, A. L. Peters, R. Pop-Busui, A. Philis-Tsimikas, S. Bao, G. Umpierrez, G. Davis, D. Kruger, A. Bhargava, L. Young, J. M. McGill, G. Aleppo, Q. T. Nguyen, I. Orozco, W. Biggs, K. J. Lucas, W. H. Polonsky, J. B. Buse, D. Price & R. M. Bergenstal, "Effect of continuous glucose monitoring on glycemic control in patients with type 2 diabetes treated with basal insulin: a randomized clinical trial", JAMA **325** (2021) 2262. https://doi.org/10.1001/jama.2021.7444.

[3] J. T. Kelly, K. L. Campbell, E. Gong & P. Scuffham, "The Internet of Things: impact and implications for health care delivery", Journal of Medical Internet Research **22** (2020) e20135. https://doi.org/10.2196/20135.

[4] S. Heydari & Q. H. Mahmoud, "Tiny Machine Learning and on-device inference: a survey of applications, challenges, and future directions", Sensors **25** (2025) 3191. https://doi.org/10.3390/s25103191.

[5] S. S. Saha, S. S. Sandha & M. Srivastava, "Machine learning for microcontroller-class hardware: a review", IEEE Sensors Journal **22** (2022) 21362. https://doi.org/10.1109/JSEN.2022.3210773.

[6] M. Horowitz, *Computing's energy problem (and what we can do about it)*, Proceedings of the 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers, San Francisco, CA, USA, 2014, p. 10. https://doi.org/10.1109/ISSCC.2014.6757323.

[7] Y. Chen, X. Dai, M. Liu, D. Chen, L. Yuan, and Z. Liu, *Dynamic convolution: attention over convolution kernels*, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 2020, p. 11083. https://doi.org/10.48550/arXiv.1912.03458.

[8] J. Zhang, X. Tang, Y. Yang, C. Ying, Y. Zhang & N. Han, "Enhancing network intrusion detection with adaptive spatial convolution and salient contrastive learning", Computer Networks **281** (2026) 112226. https://doi.org/10.1016/j.comnet.2026.112226.

[9] A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, A. Wajahat & M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem", Ain Shams Engineering Journal **15** (2024) 102777. https://doi.org/10.1016/j.asej.2024.102777.

[10] W. Ishtiaq, A. Zannat, A. H. M. S. Parvez, M. A. Hossain, M. H. Kanchan & M. M. Tarek, "CST-AFNet: a dual attention-based deep learning framework for intrusion detection in IoT networks", Array **27** (2025) 100501. https://doi.org/10.1016/j.array.2025.100501.

[11] A. Harshavardhan, M. S. Vani, A. Patil, N. Yamsani & K. Archana, "Hybrid deep learning framework for intrusion detection: integrating CNN, LSTM, and attention mechanisms to enhance cybersecurity", Journal of Theoretical and Applied Information Technology **103** (2025) 63. https://doi.org/10.5281/zenodo.15246084.

[12] A. Gueriani, H. Kheddar & A. C. Mazari, "Enhancing IoT security with CNN and LSTM-based intrusion detection systems", arXiv preprint, arXiv:2405.18624 (2024). https://doi.org/10.48550/arXiv.2405.18624.

[13] T. N. Ghorsad & A. V. Zade, "Hybrid CNN+LSTM deep learning model for intrusions detection over IoT environment", International Journal on Recent and Innovation Trends in Computing and Communication **11** (2023) 1. https://doi.org/10.17762/ijritcc.v11i10s.7588.

[14] P. Sinha, D. Sahu, S. Prakash, T. Yang, R. S. Rathore & V. K. Pandey, "A high performance hybrid LSTM-CNN secure architecture for IoT environments using deep learning", Scientific Reports **15** (2025) 9684. https://doi.org/10.1038/s41598-025-94500-5.

[15] P. Phalaagae, A. M. Zungeru, A. Yahya, B. Sigweni & S. Rajalakshmi, "A hybrid CNN-LSTM model with attention mechanism for improved intrusion detection in wireless IoT sensor networks", IEEE Access **13** (2025) 57322. https://doi.org/10.1109/ACCESS.2025.3555861.

[16] M. S. Alshehri, O. Saidani, F. S. Alrayes, S. F. Abbasi & J. Ahmad, "A self-attention-based deep convolutional neural networks for IIoT networks intrusion detection", IEEE Access **12** (2024) 45762. https://doi.org/10.1109/ACCESS.2024.3380816.

[17] D. M. A. A. Afraji, J. Lloret & L. Peñalver, "An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture", Computation **13** (2025) 222. https://doi.org/10.3390/computation13090222.

[18] A. S. Mirkhail & Z. Xinyou, "Deep learning for anomaly detection in IoT healthcare systems", International Research Journal of Multidisciplinary Scope **6** (2025) 1480. https://doi.org/10.47857/irjms.2025.v06i02.03768.

[19] N. Imtiaz, A. Wahid, S. Z. U. Abideen, M. M. Kamal, N. Sehito, S. Khan, B. S. Virdee, L. Kouhalvandi & M. Alibakhshikenari, "A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks", Photonics **12** (2025) 35. https://doi.org/10.3390/photonics12010035.

[20] A. Momand, S. U. Jan & N. Ramzan, "ABCNN-IDS: attention-based convolutional neural network for intrusion detection in IoT networks", Wireless Personal Communications **136** (2024) 1981. https://doi.org/10.1007/s11277-024-11260-7.

[21] M. Sajid, K. R. Malik, A. Almogren, T. S. Malik, A. H. Khan, J. Tanveer & A. U. Rehman, "Enhancing intrusion detection: a hybrid machine and deep learning approach", Journal of Cloud Computing **13** (2024) 123. https://doi.org/10.1186/s13677-024-00685-x.

[22] V. Kantharaju, H. Suresh, M. Niranjanamurthy, S. I. Ansarullah, F. Amin & A. Alabrah, "Machine learning based intrusion detection framework for detecting security attacks in Internet of Things", Scientific Reports **14** (2024) 30275. https://doi.org/10.1038/s41598-024-81535-3.

[23] F. S. Alsubaei, "Smart deep learning model for enhanced IoT intrusion detection", Scientific Reports **15** (2025) 20577. https://doi.org/10.1038/s41598-025-06363-5.

[24] A. M. Alashjaee, "Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection", Scientific Reports **15** (2025) 21856. https://doi.org/10.1038/s41598-025-07706-y.

[25] H. Zhang, "Development of an intelligent intrusion detection system for IoT networks using deep learning", Discover Internet of Things **5** (2025) 74. https://doi.org/10.1007/s43926-025-00177-7.

[26] B. Omarov, Z. Sailaukyzy, A. Bigaliyeva, A. Kereyev, L. Naizabayeva & A. Dautbayeva, "One-dimensional Conv-BiLSTM network with attention mechanism for IoT intrusion detection", Computers, Materials & Continua **77** (2023) 3765. https://doi.org/10.32604/cmc.2023.042469.

[27] F. Malik, "IoT Healthcare Security Dataset", Kaggle, 2024. Available online: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset.

[28] Canadian Institute for Cybersecurity, "CICIoMT-2024: a comprehensive multi-protocol Internet of Medical Things (IoMT) security dataset", University of New Brunswick, 2024. Available online: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.

[29] M. A. Talukder, M. M. Islam, M. A. Uddin, K. F. Hasan, S. Sharmin, S. A. Alyami & M. A. Moni, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction", Journal of Big Data **11** (2024) 33. https://doi.org/10.1186/s40537-024-00886-w.

[30] K. C. Santos, R. S. Miani & F. d. O. Silva, "Evaluating the impact of data preprocessing techniques on the performance of intrusion detection systems", Journal of Network and Systems Management **32** (2024) 36. https://doi.org/10.1007/s10922-024-09813-z.

[31] G. S. Vidhya & R. Nagarajan, "A novel bidirectional LSTM model for network intrusion detection in SDN-IoT network", Computing **106** (2024) 2613. https://doi.org/10.1007/s00607-024-01295-w.

[32] I. Yoon, J. Mun & K.-S. Min, "Comparative study on energy consumption of neural networks by scaling of weight-memory energy versus computing energy for implementing low-power edge intelligence", Electronics **14** (2025) 2718. https://doi.org/10.3390/electronics14132718.