RemoteCare: AI-Driven Multimodal Predictive Framework With Blockchain for Personalized Remote Patient Monitoring in IoMT

Chigozie Athanasius Nnadiekwe, Simeon Okechukwu Ajakwe, *Senior Member, IEEE*, Jae-Min Lee, *Member, IEEE*, and Dong-Seong Kim, *Senior Member, IEEE*

***Abstract*—The Internet of Medical Things (IoMT) enables continuous health monitoring but still faces challenges in achieving personalized predictions and ensuring secure, tamper-proof data integrity. We present *RemoteCare*, an AI-driven multimodal framework that fuses synchronized physiological and network data for dual-task learning, simultaneously performing personalized health state classification (normal, warning, and critical) and cyberattack detection in IoMT traffic. Unlike conventional population-based thresholds, *RemoteCare* dynamically adapts alerts to each patient's baseline, thereby minimizing false alarms and enhancing clinical reliability. A hybrid convolutional neural network (CNN)–gated recurrent unit (GRU)–long short-term memory (LSTM) architecture jointly captures spatial and temporal dependencies across heterogeneous signals, while Shapley additive explanations (SHAPs)-based explainability provides transparent, patient-specific insights into the features influencing each prediction. To guarantee auditability, all predictions are immutably recorded on the *PureChain* blockchain integrated with interplanetary file system (IPFS), ensuring decentralized and tamper-proof storage. Evaluated on the WUSTL-EHMS-2020 dataset (enhanced healthcare monitoring system), *RemoteCare* achieved 99.7% accuracy for health classification and 96.0% for intrusion detection, with negligible false alarms and efficient inference suitable for real-time deployment. By unifying multimodal prediction, personalization, interpretability, and secure logging, *RemoteCare* establishes a trustworthy framework for early intervention, patient-specific risk assessment, and clinician-oriented decision support in remote healthcare.**

***Index Terms*—Acute distress detection, blockchain-based prediction logging, cyberattack detection, edge computing in healthcare, explainable artificial intelligence (XAI), Internet of Medical Things (IoMT), multimodal data fusion, personalized medicine, real-time monitoring.**

Received 4 September 2025; revised 21 October 2025; accepted 12 November 2025. Date of publication 17 November 2025; date of current version 26 January 2026. This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 20%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 20%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 20%), and by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 20%), and by the Gyeongsangbuk-do RISE (Regional Innovation System Education) project (Regional Growth Innovation LAB unit) (20%). *(Corresponding author: Dong-Seong Kim.)*

Chigozie Athanasius Nnadiekwe, Jae-Min Lee, and Dong-Seong Kim are with the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: cnnadiekwe01@gmail.com; ljmpaul@kumoh.ac.kr; dskim@kumoh.ac.kr).

Simeon Okechukwu Ajakwe is with the ITC Convergence Research Centre, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: simeonajlove@gmail.com).

Digital Object Identifier 10.1109/JIOT.2025.3633505

NOMENCLATURE

AI	Artificial intelligence.
ABI	Application binary interface.
CNN	Convolutional neural network.
GRU	Gated recurrent unit.
LSTM	Long short-term memory.
IoMT	Internet of Medical Things.
IDS	Intrusion detection system.
IPFS	Interplanetary file system.
RF	Random forest.
SVM	Support vector machine.
DQN	Deep Q-network.
XGB	Extreme gradient boosting.
XAI	Explainable AI.
SHAPs	Shapley additive explanations.
EHR	Electronic health record.
SYS	Systolic blood pressure.
SpO_2	Peripheral capillary oxygen saturation.
PR	Pulse rate.
NEWS	National early warning score.
TPS	Transactions per second.
PoS	Proof of stake.
PoA2	Proof of authority and association.
FAR	False alarm rate.
TPR	True positive rate (sensitivity).
PPV	Positive predictive value (precision).
$X^{(n)} \in \mathbb{R}^{T \times F_n}$	Network input sequence (length T and F_n features).
$X^{(h)} \in \mathbb{R}^{T \times F_h}$	Physiological input sequence (length T and F_h features).
$y^{(a)}$	Attack label (0 = benign and 1 = attack).
$\hat{y}^{(a)}$	Predicted attack label.
$y^{(h)}$	Health state label (normal, warning, and critical).
$\hat{y}^{(h)}$	Predicted health state.
TP, FP, TN, FN	True/false positives and true/false negatives.
Accuracy	$\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{TN}+\text{FN}}$.
Precision	$\frac{\text{TP}}{\text{TP}+\text{FP}}$.
Recall (Sensitivity)	$\frac{\text{TP}}{\text{TP}+\text{FN}}$.
$F1$-score	$\frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision}+\text{Recall}}$.

L	Multitask loss function.
α, β	Loss weights for attack and health tasks.

I. Introduction

THE convergence of IoMT and intelligent data analytics is transforming healthcare delivery by enabling continuous physiological monitoring, patient-specific risk prediction, and personalized treatment interventions [1], [2]. IoMT systems integrate wearable sensors, embedded devices, and edge/cloud analytics to collect and process diverse signals such as heart rate, oxygen saturation (SpO_2), respiratory rate, and blood pressure. When enhanced with AI-driven multimodal fusion, these systems move beyond generic anomaly detection by capturing patient-specific baselines and deviations, thereby tailoring predictions to the individual rather than the population average [3], [4].

This personalization is clinically critical. Generic threshold-based systems often misclassify patients with chronic conditions, such as chronic obstructive pulmonary disease (COPD) or hypertension. These errors generate excessive false alarms, leading to alarm fatigue. In remote monitoring, this fatigue can cause caregivers to overlook true emergencies. By dynamically adapting to individual baselines, personalized monitoring reduces false alarms, preserves clinical trust, and ensures that alerts are meaningful and actionable. Moreover, for chronic care management, patient-specific trends provide early warning of deterioration that may be invisible when compared only to population norms. Thus, personalization not only improves sensitivity and specificity but also enhances long-term disease management and patient safety. This paradigm is especially vital in high-risk or resource-constrained environments, such as remote healthcare settings and military operations, where early warnings and rapid interventions can reduce morbidity and mortality [5], [6].

Despite these advances, IoMT deployments face two tightly coupled challenges: 1) ensuring robust and explainable *health state prediction* from heterogeneous physiological streams and 2) safeguarding IoMT infrastructures against *cyber threats*, including spoofing, denial-of-service (DoS), and data tampering [7], [8]. While recent multimodal frameworks demonstrate improved health prediction by fusing wearable, imaging, and EHR data [9], [10], [11], few approaches jointly consider cybersecurity as an equally critical component of remote monitoring. Conversely, IoMT IDSs have advanced from classical machine learning [7], [12] to hybrid deep learning models, including CNN–LSTM [13], [14] and ensemble learning [15], [16], yet they rarely integrate patient health modeling, limiting their clinical applicability.

In parallel, XAI has emerged as a cornerstone of trustworthy decision-making [17]. SHAP explanations serve as a clinical interpretability layer: rather than providing abstract feature weights, they highlight why the system flagged a patient at risk in a specific moment [18]. For example, SHAP can show that an alert was primarily driven by an abnormal respiratory rate combined with a network anomaly [19]. This allows clinicians to validate model reasoning against their medical knowledge, enhancing trust and enabling faster, more confident decision-making. However, most XAI-enabled systems focus on a single domain (either health or security), lacking unified interpretability for dual predictions. Similarly, blockchain technologies have been proposed for secure IoMT logging, ensuring data integrity, access control, and auditability [7], [20], [21], but these frameworks often restrict recording to security alerts and neglect health outcomes, thereby offering incomplete transparency in clinical decision support.

The state of the art reveals a pressing gap: there is no holistic, multimodal IoMT framework that integrates health monitoring, cyberattack detection, explainable outputs, and decentralized logging into a single real-time system. To address this, we propose *RemoteCare*, an AI-driven multimodal framework for personalized healthcare and secure remote monitoring. RemoteCare fuses physiological and network features using a hybrid CNN–GRU–LSTM architecture for dual-task classification. SHAP-based explainability is applied to both health and intrusion predictions, providing clinicians and analysts with transparent insights. Finally, predictions are immutably recorded on the *PureChain* blockchain with role-based access control, while supplementary evidence is distributed via IPFS for tamper-proof archiving. This end-to-end design advances the field toward trustworthy, personalized, and resilient remote patient monitoring.

The key contributions of this work are as follows.

1) *Dual-Task Classification:* A unified deep learning pipeline that simultaneously performs health state classification (normal, warning, and critical) and multiclass cyberattack detection from synchronized IoMT data streams.
2) *Hybrid Deep Learning Architecture:* A CNN–GRU–LSTM model that captures both spatial feature patterns and long-term temporal dependencies for robust anomaly detection in physiological and network data.
3) *Holistic Explainability:* Application of SHAP to both health and security predictions, enabling interpretable, context-aware decision support.
4) *Blockchain-Enabled Auditability:* Integration of the PureChain blockchain and IPFS to provide immutable, decentralized logging of all predictions, with role-based access control for secure retrieval.

By addressing the intertwined challenges of health prediction, network intrusion detection, explainability, and data integrity in a single system, *RemoteCare* advances the state of the art in secure, transparent, and reliable IoMT monitoring.

The rest of this article is organized as follows. Section II explores previous approaches and provides insights about existing gaps addressed. Section III presents the system architecture and methodology; Section IV discusses experimental results and performance evaluation; and Section V concludes the study with future directions.

II. Literature Review

Recent research on IoMT security and monitoring has evolved along two largely parallel tracks: *physiological health*

prediction and *network intrusion detection*. Early health monitoring systems, such as those by Jayant et al. [5] and Wong et al. [6], relied on wearable sensors and basic anomaly detection (e.g., static thresholds and simple ML) to detect deviations in patient vitals. While these approaches provided end-to-end monitoring, they lacked network security capabilities, explainability, and blockchain integration. More advanced systems, such as Shamout et al.'s DEWS [25] and Sung et al. [26], applied deep sequence models (Bi-LSTM and attention) to capture long-term dependencies in physiological data, but did not address cybersecurity. Parallel progress in IDS for IoMT includes Goumidi and Pierre [15] with a stacking meta-learner on a proprietary healthcare dataset, Ajakwe et al. [13] using ensemble AI for high-accuracy detection, and Daher [22] applying deep Q-learning for DDoS classification. While Kavkas and Yildiz [23] demonstrated multiclass attack detection with DNN and LSTM, and Benmalek et al. [16] proposed a stacked ensemble (CNN, LSTM, GRU, and DNN) for the WUSTL-EHMS-2020 dataset, these efforts remain focused solely on cyber threats, without integrating patient health monitoring.

A subset of works combines AI with XAI for interpretability. Alani et al. [17] applied an explainable ensemble (RF, DT, SVC, and XGB) to IoMT cyberattack detection on WUSTL-EHMS-2020, using SHAP for feature attribution, while Kalakoti et al. [18] and Binsar and Sasmoko [19] explored XAI in IDS and healthcare systems for transparency and trust. However, these XAI integrations are typically confined to intrusion detection, with no dual-domain health and attack coverage. Ravi et al. [14] demonstrated that combining biometric and network features with a CNN–LSTM improves IDS accuracy, yet their model lacked blockchain and XAI. Hady et al. [8] created a real-time EHMS testbed combining medical and network data, but did not implement explainability or on-chain verification. Other AI-based IDS models, such as Nandy et al. [24] using a swarm neural network, also omit XAI. These limitations highlight the lack of real-time, explainable, dual-task AI in current literature.

Blockchain has emerged as a tool for ensuring integrity, privacy, and auditability in IoMT, particularly for IDS. Olawale and Ebadinezhad [7] compared classical ML and DL models for anomaly detection using datasets, such as TON_IoT, Edge_IIoT, and UNSW-NB15, securing results on-chain and via IPFS, but without health prediction or XAI. Aljuhani [20] proposed a blockchain-empowered collaborative IDS for IoMT with multisite sharing, yet lacked practical deployment detail and explainability. Gupta et al. [12] developed a blockchain-based coalition framework for IDS in heterogeneous IoMT networks, but did not integrate physiological anomaly detection. Zaabar et al. [27] combined Hyperledger Fabric with federated learning for decentralized IDS model aggregation, while Tyagi et al. [21] reviewed blockchain solutions for IoMT cybersecurity. Despite these efforts, most blockchain-enabled IDSs focus on cyber events only, lack XAI, and omit real-time role-based access to unified health–attack predictions.

The proposed *RemoteCare* framework addresses these gaps by unifying *dual-task AI*, *holistic XAI*, and *blockchain-secured auditability* in a real-time IoMT pipeline. Its hybrid CNN–GRU–LSTM architecture extracts spatiotemporal features from synchronized physiological and network streams, enabling simultaneous health state classification and intrusion detection. Unlike prior works, SHAP is applied to both outputs, providing interpretability for clinicians and security analysts alike. All predictions, health, and attack are immutably recorded on the *PureChain* network with role-based access control, while IPFS stores supplementary evidence in a tamper-proof, distributed manner. This approach resolves the key limitations in reviewed works (see Table I) by enabling multimodal prediction, ensuring full-spectrum traceability, and maintaining operational efficiency in resource-constrained IoMT environments.

III. Proposed Methodology

The *RemoteCare* framework is an end-to-end, secure, and intelligent IoMT monitoring system that combines real-time health assessment with robust data integrity verification. Wearable IoMT devices capture physiological signals (e.g., heart rate, SpO_2, respiratory rate, temperature, and blood pressure) and process them locally via a lightweight CNN–GRU–LSTM model for *multiclass health classification* (normal, warning, and critical) (see Section III-B). Critical states trigger immediate on-device alarms while waiting for caregiver confirmation, minimizing response delays Section III-B1. Preprocessed data and classification results are sent to the cloud server, where a dedicated model performs *binary network attack detection* on network flow features to confirm transmission integrity. Verified records are hashed, immutably stored on the PureChain blockchain (see Section III-C), and linked to full off-chain records in IPFS via content identifiers (CIDs). Caregivers access real-time and historical data through a secure dashboard, enabling timely interventions and feedback, which are relayed back to the patient's device. This integrated pipeline ensures continuous monitoring, rapid alerts, tamper-proof storage, and bidirectional patient–caregiver communication, as illustrated in Fig. 1. XAI feedback layer was implemented in Section III-D to understand the contribution of each input feature.

A. Dataset Description and Preprocessing

The WUSTL-EHMS-2020 dataset [8] comprises synchronized network traffic records and physiological measurements collected in an IoMT emulation environment. It contains 16 318 samples and 45 feature columns, without missing values in the processed version used for this study. The dataset provides a balanced view of IoMT operational conditions by including both benign and malicious network traffic alongside patient vital signs. This joint feature space enables simultaneous health state classification and intrusion detection.

An exploratory data analysis (EDA) was performed to inspect the dataset and verify the integrity and validity of both the network and physiological features before model training. Nonnumeric values in vital sign columns (e.g., `Resp_Rate`, SpO_2, and `Heart_rate`) were coerced to numeric, and missing entries were removed. Feature-wise range checks were conducted against clinical standards (e.g., respiratory rate

TABLE I
COMPARATIVE ANALYSIS OF REMOTECARE AND RELATED WORKS, HIGHLIGHTING GAPS

Authors	Dataset	AI Model(s)	BCN	XAI	Focus	Key Contributions	Limitations	Addressed by RemoteCare
[7]	TON_IoT, Edge_IIoT, UNSW-NB15	SVM, RF, DT, GB, CNN, LSTM, hybrid CNN-LSTM	Yes	No	Attacks	Compared classical ML and DL models for anomaly detection; on-chain/IPFS data security	Slow simulations; blockchain test complexity;	Health prediction; Real-time pipeline; SHAP explainability
[20]	Real IoMT streams	Distributed IDS	Yes	No	Attacks	Blockchain-empowered collaborative IoMT IDS; multi-site sharing	Practical deployment details and XAI missing	SHAP; role-based audit logs; on-chain predictions for traceability
[12]	Heterogeneous IoMT networks	Ensemble voting	Yes	No	Attacks	Coalition framework	Health prediction and XAI gaps	integrate both network intrusion detection and physiological anomaly detection into a single dual-output; SHAP; on-chain logging
[17]	WUSTL-EHMS-2020	Ensemble (RF + DT + SVC + XGB, soft voting)	No	Yes	Attacks	Explainable ensemble for IoMT cyber-attacks	No blockchain; dataset scope narrow	Blockchain proofs; + Health prediction; Real-time pipeline
[15]	Healthcare-specific IoMT dataset	Stacking (meta-learner over base ML)	No	No	Attacks	Real-time anomaly detection pipeline for IoMT	No blockchain / XAI; Dataset is proprietary (limits reproducibility)	Includes sliding-window preprocessing, multi-branch feature extraction, and fusion layers for decision-making
[22]	Not stated	Deep Q-Learning (+SVM baseline)	No	No	Attacks	DRL for attack classification, DDoS emphasis	No blockchain / XAI; no health status	Unify health+attack views, SHAP, and on-chain traceability
[14]	WUSTL-EHMS-2020	CNN-LSTM (DL)	No	No	Attacks	Proposed DL-based IDS for IoMT using both network and biometric data	No blockchain; no XAI; single dataset	Add PureChain logging, SHAP; multi-dataset validation
[23]	CICIoMT2024	DNN, LSTM	No	No	Attacks	Proposed DNN and LSTM for binary, six-class, and nineteen-class attack detection	No blockchain or immutable logging; No health data classification	dual attack + health classification; Integrates PureChain blockchain
[8]	WUSTL-EHMS 2020 (medical + network, testbed)	KNN, SVM, RF, etc. (comparative)	No	No	Attack	Built a real-time EHMS testbed combining medical and network features	No blockchain / XAI	Integrates dual-input deep learning, SHAP, PureChain
[24]	ToN-IoT dataset	Swarm-Neural Network (SNN)	No	No	Attacks	Proposed SNN for IoMT intrusion detection	No blockchain; limited explainability	On-chain audit + SHAP; health+attack prediction
[6]	Wearables/vitals + alerts	Thresholding, simple ML	No	No	Health	End-to-end remote monitoring	No IDS/XAI/blockchain	RemoteCare adds security IDS, explainability and on-chain logging
[5]	Patient vitals (IoT devices)	Basic anomaly rules/ML	No	No	Health	Combined monitoring + simple anomaly alerts	No network-security; no XAI/chain	Integrates IDS + SHAP + PureChain
[16]	WUSTL-EHMS-2020	Stacked ensemble of CNN, LSTM, GRU, DNN	No	No	Attack	Proposed SNN-IoMT ensemble IDS for IoMT	No blockchain integration; no XAI	Retains both health and attack classification in one architecture, SHAP, and auditable blockchain logs

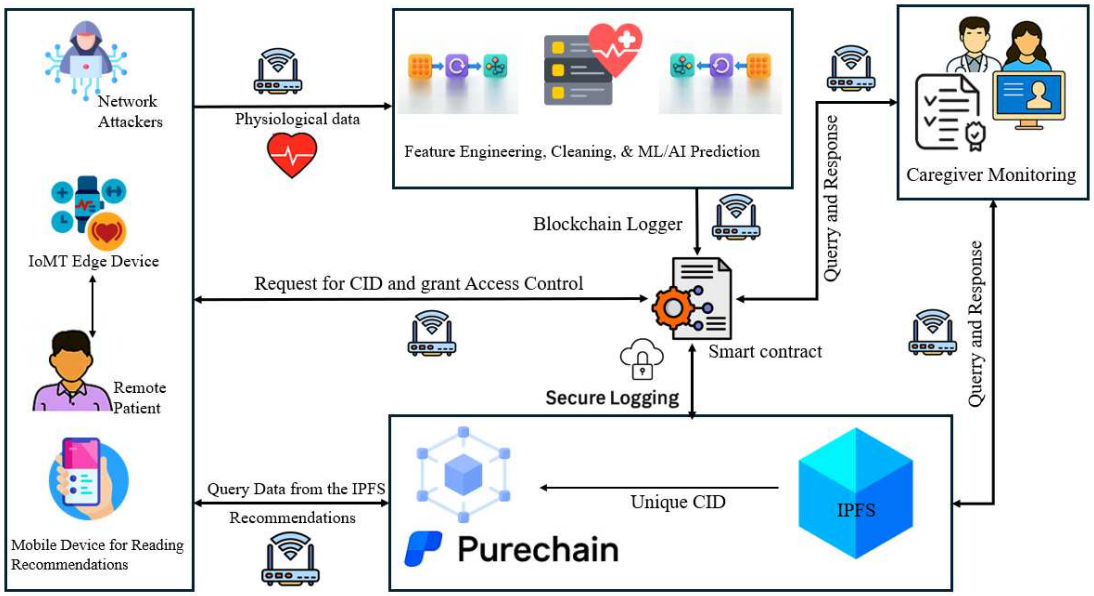

Fig. 1. Proposed system architecture for the RemoteCare, highlighting the four-tier layers: edge layer, AI cognitive and prediction layer, blockchain security layer, and explainable feedback layer.

12–20 breaths/min and oxygen saturation 95%–100%), and bar charts were plotted to compare in-range and out-of-range counts. Categorical analysis of the `Attack Category` variable revealed class imbalance between benign and malicious

TABLE II
SUMMARY OF KEY FEATURES USED IN MODEL

Domain	Top Features
Network	DIntPkt, DstJitter, Load, SrcLoad, Rate, SIntPkt, Packet_num, DstLoad, Dur, SrcJitter
Health	Heart_rate, Resp_Rate, SpO_2, Pulse_Rate, SYS

traffic. The health label assignment was formalized as

$$y_i^{(h)} = \begin{cases} 0, & \text{if all vitals are within normal ranges} \\ 1, & \text{if any vital is in a warning range} \\ 2, & \text{otherwise(critical condition)} \end{cases}$$

where $y_i^{(h)}$ denotes the health class for sample i. This preprocessing ensured that the downstream CNN–GRU–LSTM hybrid model was trained on consistent, clinically meaningful features for both binary attack detection and multiclass health classification.

For this study, the top ten network features and the top five physiological features (see Table II) were selected based on feature importance ranking. Health status labels were generated using clinically acceptable thresholds and validated against ground truth according to the NEWS [28], to categorize samples into *Normal*, *Warning*, and *Critical* classes. The original network attack labels included *Normal* and *Data Alteration*, and *Spoofing*. But for binary attack detection, the two attack categories (Data Alteration and Spoofing) were merged into a single Attack label, while Normal instances were retained as the Normal class. This binary mapping simplifies the classification task for the network anomaly detection branch, enabling the model to focus on detecting the presence or absence of malicious activity rather than differentiating between specific attack types. This transformation was implemented through categorical mapping, ensuring class balance was preserved and that both attack types were equally represented within the positive (Attack) class. Data was windowed using a sliding approach ($T = 60$ time steps) to preserve temporal dependencies, resulting in samples of shape (T, F_{net}) for network features and (T, F_{health}) for physiological features. Feature scaling (min–max normalization) was applied independently per channel.

B. Hybrid CNN–GRU–LSTM Detection and Prediction Module

Let $\mathbf{X}^{(n)} \in \mathbb{R}^{T\times F_n}$ and $\mathbf{X}^{(h)} \in \mathbb{R}^{T\times F_h}$ denote the synchronized network and physiological sequences over a window of T timesteps with F_n and F_h features, respectively. The proposed model is illustrated in Fig. 2. It comprises two parallel input branches.

1) *Network Branch:* Ten most important network traffic features.
2) *Physiological Branch:* Five physiological features (heart rate, SpO_2, respiratory rate, and so on).

A synchronized sliding window approach was used to segment both inputs into fixed-length sequences of 60 timesteps per sample, ensuring temporal alignment between physiological and network activity. It performs *dual* inference: 1) binary attack detection $\hat{y}^{(a)} \in [0, 1]$ and 2) multiclass health classification $\hat{\mathbf{y}}^{(h)} \in \Delta^{C_h-1}$ (simplex of C_h classes, here $C_h = 3$: Normal/Warning/Critical).

For the *Network Branch (CNN)*, we applied a 1-D convolution with kernel size 1 to learn local, per-timestep channel interactions, followed by a flattening and a bottleneck dense layer

$$\mathbf{H}_t^{(n)} = \sigma\left(\mathbf{W}^{(n)}\mathbf{X}_t^{(n)} + \mathbf{b}^{(n)}\right)$$
$$\mathbf{z}^{(n)} = \phi\left(\text{Flatten}\left(\mathbf{H}^{(n)}\right)\right)\mathbf{W}_{bn}^{(n)} + \mathbf{b}_{bn}^{(n)}$$

where σ is ReLU and ϕ denotes an affine layer with ReLU [the notebook uses `Conv1D(64, 1)` → `Flatten` → `Dense(32)`].

For the *Physiological Branch (GRU→LSTM)*, the temporal structure of vital signs is modeled with a GRU layer (short/medium memory) followed by an LSTM (long memory)

$$\begin{aligned}
\textbf{GRU:}\quad & z_t = \sigma(\mathbf{W}_z\mathbf{x}_t + \mathbf{U}_z\mathbf{h}_{t-1}) \\
& r_t = \sigma(\mathbf{W}_r\mathbf{x}_t + \mathbf{U}_r\mathbf{h}_{t-1}) \\
& \tilde{\mathbf{h}}_t = \tanh(\mathbf{W}_h\mathbf{x}_t + \mathbf{U}_h(r_t \odot \mathbf{h}_{t-1})) \\
& \mathbf{h}_t = (1 - z_t)\odot\mathbf{h}_{t-1} + z_t \odot \tilde{\mathbf{h}}_t \\
\textbf{LSTM:}\quad & i_t = \sigma(\mathbf{W}_i\mathbf{x}_t + \mathbf{U}_i\mathbf{h}_{t-1} + \mathbf{b}_i) \\
& f_t = \sigma\left(\mathbf{W}_f\mathbf{x}_t + \mathbf{U}_f\mathbf{h}_{t-1} + \mathbf{b}_f\right) \\
& \tilde{\mathbf{c}}_t = \tanh(\mathbf{W}_c\mathbf{x}_t + \mathbf{U}_c\mathbf{h}_{t-1} + \mathbf{b}_c) \\
& c_t = f_t \odot c_{t-1} + i_t \odot \tilde{\mathbf{c}}_t \\
& o_t = \sigma(\mathbf{W}_o\mathbf{x}_t + \mathbf{U}_o\mathbf{h}_{t-1} + \mathbf{b}_o) \\
& \mathbf{h}_t = o_t \odot \tanh(c_t).
\end{aligned}$$

The last hidden state is passed through a dense bottleneck

$$\mathbf{z}^{(h)} = \phi(\mathbf{h}_T)\,\mathbf{W}_{bn}^{(h)} + \mathbf{b}_{bn}^{(h)}$$

[the notebook uses `GRU(64, return_sequences=True)` → `LSTM(32)`].

Branch embeddings are concatenated and regularized with dropout, then projected for *Feature Fusion and Heads*

$$\mathbf{z} = \left[\mathbf{z}^{(n)};\ \mathbf{z}^{(h)}\right], \qquad \tilde{\mathbf{z}} = \text{ReLU}(\mathbf{z}\mathbf{W}_{\text{fuse}} + \mathbf{b}_{\text{fuse}})$$

followed by two task-specific heads

$$\hat{y}^{(a)} = \sigma(\tilde{\mathbf{z}}\mathbf{w}_a + b_a), \qquad \hat{\mathbf{y}}^{(h)} = \text{softmax}(\tilde{\mathbf{z}}\mathbf{W}_h + \mathbf{b}_h).$$

In code, these are `Dense(1, sigmoid)` for attack and `Dense(3, softmax)` for health.

Mathematically, the model *training objective and optimization* is defined as: given attack labels $y^{(a)} \in \{0, 1\}$ and health one-hot labels $\mathbf{y}^{(h)} \in \{0, 1\}^{C_h}$, we minimize the weighted multitask loss

$$\mathcal{L} = \alpha\,\underbrace{\text{BCE}\left(y^{(a)}, \hat{y}^{(a)}\right)}_{\text{attack}} + \beta\,\underbrace{\text{CE}\left(\mathbf{y}^{(h)}, \hat{\mathbf{y}}^{(h)}\right)}_{\text{health}}.$$

Hyperparameters were selected via empirical tuning and validation. We adopted the Adam optimizer with an initial learning rate of 0.001, as it yielded stable convergence across pilot experiments. A batch size of 256 balanced computational efficiency with gradient stability. Early stopping (patience = 10)

Algorithm 1 RemoteCare Hybrid Model for Attack Detection and Health Classification

Input: D: dataset, F_{net}: network features, F_{health}: physiological features, T_{attack}: attack label
Output: M: trained model, R_{attack}, R_{health}: evaluation metrics
while *True* **do**
  1. Feature Validation:
  if *(F_{net} not in D) or (T_{attack} not in D)* **then**
    Terminate
  end
  2. Preprocessing:
  Fill missing values in $X \leftarrow D[F_{net} \cup F_{health}]$ with mean
  $y_{attack} \leftarrow$ clean and encode binary labels
  $y_{health} \leftarrow$ rule-based classification (Normal, Warning, Critical)
  3. Normalization & Reshaping:
  Standardize features
  Reshape $X_{net} \in \mathbb{R}^{N\times 1\times |F_{net}|}$, $X_{health} \in \mathbb{R}^{N\times 1\times |F_{health}|}$
  4. Data Split:
  Perform 70/15/15 train-test-val split (stratified)
  5. Model Construction:
  Define Network branch: Conv1D $\rightarrow$ Flatten $\rightarrow$ Dense
  Define Health branch: GRU $\rightarrow$ LSTM
  Concatenate branches $\rightarrow$ Dropout $\rightarrow$ Dense
  Define Outputs: attack (sigmoid), health (softmax)
  6. Training:
  Set Loss functions: binary (attack), categorical (health)
  Set Optimizer: Adam
  Train for 50 Epochs, Batch size 32, with Early stopping
  7. Evaluation:
  Predict $\hat{y}_{attack}$, $\hat{y}_{health}$
  Compute accuracy, precision, recall, F1-score
  Generate confusion matrices
end

and dropout (0.5) were applied to prevent overfitting. To ensure both tasks contributed equitably, the weights α and β were tuned using a small grid search over values $\{0.25, 0.5, 1.0\}$. The configuration $\alpha = 1$ and $\beta = 1$ achieved the best trade-off between intrusion detection and health classification on the validation set, avoiding dominance of one task over the other while preserving overall robustness.

At test time (*inference*), both branches consume their respective sequences and produce joint predictions $(\hat{y}^{(a)}, \hat{\mathbf{y}}^{(h)})$. We threshold $\hat{y}^{(a)}$ at 0.5 for the binary decision and select arg max over $\hat{\mathbf{y}}^{(h)}$ for the health state. Confusion matrices and per-class metrics (precision/recall/F1), along with accuracy and AUC (binary head), are computed on the held-out set.

To implement the CNN–GRU–LSTM model, we defined two `Input` tensors with shapes (T, F_n) and (T, F_h), as described in Algorithm 1 (with $T = 1$ and 60 timesteps supported by the layers used). The network branch uses `Conv1D(64, kernel_size=1)` $\rightarrow$ `Flatten` $\rightarrow$ `Dense(32)`; and the physiological branch uses `GRU(64, return_sequences=True)` $\rightarrow$ `LSTM(32)`. After concatenation, a `Dropout(0.5)` and `Dense(64)` layer form the fused representation. Two output layers are defined: `Dense(1, activation='sigmoid', name='attack_output')` and `Dense(3, activation='softmax', name='health_output')`. Predictions are produced as `pred_attack, pred_health = model.predict([Xn_test, Xh_test])`, then binarized/argmaxed for reporting.

*Rationale for Hybrid Integration:*We combined CNN, GRU, and LSTM layers to capture complementary aspects of IoMT data. CNN layers efficiently extract spatial and local feature patterns from high-dimensional network traffic. GRUs capture medium-term temporal dependencies in physiological sequences with fewer parameters than LSTMs, reducing training cost. LSTMs to model long-term dependencies and gradual trends in vital signs, which are critical for detecting early health deterioration. This hybrid integration ensures that both short-lived anomalies(e.g., sudden network spikes (spoofing traffic bursts) or abrupt heart rate changes) and long-term temporal patterns are learned within a unified framework, improving robustness for dual-task prediction.

1) Distress Prediction Based on Rule-Based Health Categorization: To complement the deep learning-based anomaly detection framework, we implemented a *rule-based distress prediction module* that categorizes patient health status into three discrete classes: *Normal (0)*, *Warning (1)*, and *Critical (2)*. The classification relies on predefined physiological thresholds derived from established clinical guidelines, such as the NEWS [28], thereby enabling rapid decision-making when real-time vital signs deviate from expected norms without requiring computationally intensive models. In practice, baseline vitals are individualized by profiling each patient's historical trends. Instead of applying one-size-fits-all thresholds, RemoteCare recalibrates risk zones per patient. For example, a COPD patient with consistently low SpO_2 will trigger alerts only when values drop significantly from their personal baseline, rather than being misclassified by general population standards. This ensures precision in monitoring and reduces false positives, aligning predictions with clinical reality.

The categorization is performed by evaluating incoming physiological parameters, *pulse rate* (Pulse_Rate), *oxygen saturation* (SpO_2), *heart rate* (Heart_Rate), SYS, and *respiratory rate* (Resp_Rate), against three sets of rules.

a) Normal condition (class 0): All parameters fall within standard healthy ranges.

(i) Temp: 36.1 °C–37.8 °C.
(ii) SpO_2: $\geq$ 95%.
(iii) HR: 60–100 bpm.
(iv) SYS: 90–120 mmHg.
(v) Resp_Rate: 12–20 breaths/min.

b) Warning condition (class 1): Mild deviations from the normal range, such as

(i) Temp: 35.0 °C–36.0 °C or 37.9 °C–38.5 °C.
(ii) SpO_2: 90%–95%.
(iii) HR: 50–60 or 100–110 bpm.
(iv) SYS: 80–85 or 125–130 mmHg.
(v) Resp_Rate: 10–12 or 21–24 breaths/min.

c) Critical condition (class 2): Any reading outside the above two categories is flagged as critical, indicating potential medical emergencies, such as hypoxia, hyperthermia, hypotension, or severe bradycardia/tachycardia. The function implementation employs NumPy's vectorized conditional selection to evaluate all incoming measurements efficiently, enabling real-time classification of streaming IoMT data. This categorization serves as the *distress prediction* output in the hybrid model, providing an interpretable, low-latency safety

layer to detect and escalate physiological anomalies before severe deterioration occurs.

2) Alarm System for Distress Prediction: To enhance the operational readiness of RemoteCare beyond offline classification, we integrated a real-time alarm subsystem that continuously monitors physiological predictions from the health classification branch of the CNN–GRU–LSTM model. Employing a sliding-window strategy, the system processes consecutive segments of synchronized physiological data and raises a *critical* alert whenever the predicted probability of a severe health condition surpasses a predefined threshold. Each alarm event is automatically logged with its associated prediction confidence and timestamp, enabling both immutable on-chain recording via the PureChain blockchain and secure local archival for retrospective analysis. This dual-logging design facilitates precise identification of *false alarms* (critical alerts without ground-truth distress) and *missed distress* (ground-truth distress without an alarm) in real time.

C. PureChain–IPFS Tamper-Proof Integrated Architecture

To ensure immutable, verifiable, and cost-efficient prediction tracking, the RemoteCare framework employs a blockchain–IPFS architecture deployed on the PureChain network. This decentralized infrastructure ensures data integrity and auditability while incorporating advanced security features [29]. PureChain is a purpose-built blockchain ecosystem engineered to address the fundamental quad-lemma constraints of decentralization, security, scalability, and transaction cost efficiency [30]. PureChain offers features such as zero gas costs, easy-to-use, intuitive API, full EVM support, readable Python code, secure industry-standard cryptography, account management, Python-friendly compilation, and deployment.

1) Blockchain Logging Layer: At the core of this blockchain integration is the `PredictionLogger` smart contract, implemented in Solidity on the OpenZeppelin `AccessControl` framework. The contract defines a `LOGGER_ROLE`, derived via `keccak256`, to enforce strict, role-based access control. Only authorized devices can invoke the `logPrediction()` function, which emits a `PredictionLogged` event containing the following.

i) The sender's blockchain address (ensuring traceability).
ii) An immutable block timestamp (providing chronological ordering).
iii) Serialized attack and health predictions stored as `bytes` (ensuring format flexibility).

This event-based design ensures tamper-evident, timestamped, and publicly verifiable records of predictions. The constructor() was employed to grant both administrative and logging rights to the deployer, establishing secure governance from initialization.

2) On-Chain Logging via PureChain Configuration: The setup loads RPC_URL, PRIVATE_KEY, CONTRACT_ADDRESS, and ABI_PATH from.env; initializes Web3; the ABI was built by compiling the smart contract. Small-size, single-instance predictions are transmitted to the `PredictionLogger` smart contract on the PureChain blockchain using a Python/Web3 pipeline.

Algorithm 2 State-Based Role-Controlled Logging in PureChain

Input: Predictions $(\hat{y}^{(a)}, \hat{y}^{(h)})$, Gateway G, Contract C, IPFS
Output: On-chain `PredictionLogged`event, optional IPFS CID
State 0: Initialization
Grant `DEFAULT_ADMIN_ROLE`and `LOGGER_ROLE`to Admin A
Authorize Gateway G with `LOGGER_ROLE`
State 1: Encode Payload
Serialize predictions → bytes (*attack*, *health*)
If payload size > threshold: upload full record to IPFS → CID
State 2: Verify Role
If $G \notin$ `LOGGER_ROLE`: reject transaction
Else: proceed
State 3: Log Prediction
Emit `PredictionLogged(G, timestamp, attack, health)`
Record hash on-chain; link CID if available

The contract, secured with role-based access control (`LOGGER_ROLE`), normalizes to JSON, encodes each payload as UTF-8 bytes, immutably records the prediction metadata on-chain, and emits a `PredictionLogged` event for immediate retrieval. PureChain's proof-of-authority-and-association (PoA^2) consensus ensures efficient transaction mining with zero transaction fees and low-latency confirmation.

*Role-Based Access Control:*The PredictionLogger contract enforces strict role-based access using OpenZeppelin's`AccessControl` module. Only accounts assigned the `LOGGER_ROLE` can invoke the `logPrediction()` function, ensuring that only authenticated IoMT gateways record predictions on-chain. The simplified pseudocode Algorithm 2 illustrates this mechanism.

This design guarantees that only authorized devices can emit immutable, timestamped events, preventing unauthorized access or tampering. Thus, enabling real-time high-frequency logging without economic or performance constraints.

3) Off-Chain Storage via IPFS: The larger datasets, such as aggregated prediction logs and detailed historical analysis files, are stored in IPFS. Upon upload, IPFS returns a unique CID that cryptographically represents the file's contents. Instead of storing the file itself on-chain, only the CID is recorded in the blockchain transaction, creating a tamper-evident, verifiable link between on-chain entries and off-chain content. Retrieval involves querying the blockchain for the CID and fetching the data from IPFS, where the hash is verified to confirm authenticity.

4) Patient-Centric Access Control: Patient data governance is embedded into the system via blockchain-based access management. Patients or authorized administrators can grant or revoke caregiver access by updating role assignments in the smart contract. Caregivers with valid credentials can retrieve

prediction results through event logs and by resolving IPFS CIDs linked on-chain. This ensures that only trusted entities can access sensitive health information while maintaining a complete and immutable audit trail of all access and updates.

5) Real-Time Visualization and Analytics: The front-end monitoring dashboard subscribes to blockchain event listeners, enabling instantaneous updates upon new prediction logs. For historical or aggregated insights, the dashboard retrieves CID-linked files from IPFS and merges them with on-chain data, providing both real-time alerts and long-term analytics in a unified view. By integrating blockchain's immutability and auditability with IPFS's distributed storage scalability, RemoteCare achieves secure, transparent, and patient-controlled logging for IoMT-based health and cyberattack monitoring. This design ensures immediate operational awareness, resilient long-term storage, and granular access control—critical in clinical and high-risk operational environments.

D. XAI Feedback Layer for Interpretable Monitoring

To enhance interpretability of feedback, we integrated SHAPs into the *RemoteCare* CNN–GRU–LSTM model to quantify the contribution of input features in both the network and health classification branches. Also, the XAI layer provides a human-like (anthropomorphic) explanation of the reasons for the model's prediction, which guides both the end-user and other stakeholders in taking expert-based and factual decisions. After model training, SHAP's `DeepExplainer` is applied directly to the Keras model, yielding both local and global explanations. SHAP values provide localized, patient-specific interpretability—identifying which features drive a distress prediction for a given individual. This personalization is crucial for clinicians, who can trace each alarm to physiologically relevant factors for that patient.

For a given sample x, SHAP estimates the marginal contribution of each feature by comparing the model's output when the feature is present versus when it is replaced by a baseline value (e.g., mean or zero). The Shapley value for feature i is defined as

$$\phi_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|!\,(|F| - |S| - 1)!}{|F|!} \left[f_{S\cup\{i\}}\left(x_{S\cup\{i\}}\right) - f_S\left(x_S\right) \right]$$

where

1) F is the set of all features;
2) S is a subset of features not containing i;
3) $f_S(x_S)$ is the model prediction using only features in S; and
4) ϕ_i is the Shapley value for feature i.

In our implementation:

1) *Background Data:* A representative subset of the training set was used to approximate the expected feature distribution.
2) *Branch-wise Explanation:* SHAP was applied separately to the network branch (CNN) and health branch (GRU–LSTM), as well as to the fused final output.
3) *Visualization:* Summary plots highlighted global feature rankings (see Section IV-E).

TABLE III
CNN–GRU–LSTM MODEL PARAMETERS

Parameter	Value
Input window size (T)	60
Network branch: CNN filters	64 (kernel size = 1)
Network branch: GRU units	64
Health branch: LSTM units	32, stacked
Fusion layer (Dense)	64
Dropout (fusion)	0.5
Attack output activation	Sigmoid
Health output activation	Softmax
Optimizer	Adam (lr = 0.001)
Batch size	256
Epochs	100
Early stopping patience	10
Loss function	Categorical cross-entropy

This approach enables transparent decision-making by revealing, for example, that high `DstJitter` values significantly contribute to attack detection, while low SpO_2 readings are primary indicators for triggering critical health alerts.

E. Experimental and Simulation Setup

For the experimental and simulation setup, the details of the model's principal architecture and training parameters are captured in Table III.

Regularization (dropout and early stopping) and learning rate scheduling were applied to maximize generalization. Model selection was based on the validation set macro-$F1$ score. The WUSTL-EHMS-2020 dataset was split 70%/15%/15% into train, validation, and test partitions, ensuring all classes were represented. The model performance was assessed using various metrics, such as accuracy, precision, recall, $F1$ score, FAR, missed detection rate, and average inference time. The definitions of these metrics are captured in the list of acronyms (see Nomenclature). Model training and evaluation were conducted on a workstation equipped with an Intel Core i9-12900K CPU @ 3.20 GHz, 64 GB RAM, and an NVIDIA RTX 3090 GPU with 24 GB VRAM, running Ubuntu 22.04 LTS. The implementation was developed in Python 3.10 using TensorFlow/Keras 2.11, Scikit-learn 1.2, and SHAP 0.41. Blockchain integration for on-chain logging was performed using the PureChain network (PoA^2 consensus and zero transaction fee), with smart contracts implemented in Solidity 0.8.20 and deployed via the Hardhat framework. Web3.py 6.0 was used for blockchain interaction, and all experiments were repeated three times to ensure result stability.

IV. RESULTS DISCUSSION AND PERFORMANCE EVALUATION

This section evaluates our proposed *RemoteCare* framework for remote patient monitoring to detect real-time acute distress and cyberattack prediction. The evaluation focuses on both the physiological anomaly detection (see Section IV-A) and the network intrusion detection components (see Section IV-C), as well as the overall performance of the integrated hybrid CNN–GRU–LSTM model. We present results for accuracy, precision, recall, and $F1$-score across both tasks, supported by confusion matrices to illustrate class-wise performance.

TABLE IV
WEIGHTED AVG OF REMOTECARE HEALTH CLASSIFICATION PERFORMANCE VERSUS BASELINE MODELS

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	0.961	0.95	0.96	0.95
CNN-LSTM	0.982	0.98	0.98	0.98
LSTM	0.980	0.98	0.98	0.98
SVM	0.917	0.97	0.92	0.94
RF-CNN-GRU-LSTM	0.983	0.98	0.98	0.98
CNN	0.980	0.98	0.98	0.98
RemoteCare	0.997	1.00	0.99	1.00

TABLE V
REMOTECARE ALARM SYSTEM EVALUATION METRICS

Metric	**Description**	**Result**
Total Test Samples	Sliding-window instances evaluated in test phase	31,830
True Distress Windows	Windows containing actual health distress events	342
False Alarms	Alarm triggered when no distress was present	8
Missed Distress	Distress occurred but no alarm triggered	0
False Alarm Rate (FAR)	[False Alarms] / [Total Non-Distress]	0.000
Miss Rate	[Missed Distress] / [True Distress]	0.000
Sensitivity (TPR)	TP / (TP+FN)	1.000
Precision (PPV)	TP / (TP+FP)	0.977

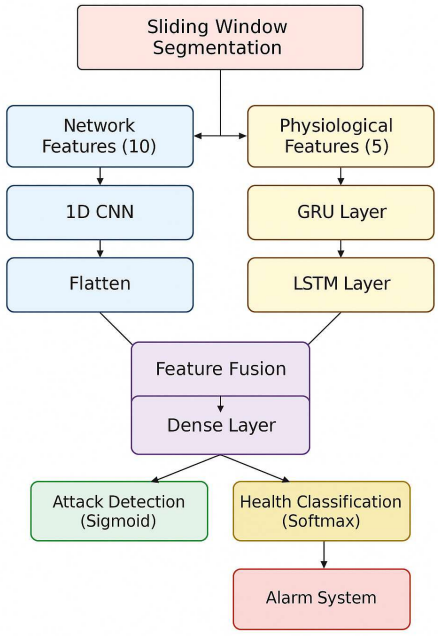

Fig. 2. Proposed CNN–GRU–LSTM architecture for joint attack and health classification in RemoteCare.

In addition, we evaluate the system's alarm mechanism (see Section IV-B) for the timely identification of critical health states, measuring key metrics, such as FAR, miss rate, sensitivity, and precision, in critical event detection. To validate the security layer, we report blockchain logging performance (see Section IV-D), including transaction latency, throughput, and gas cost on both Ethereum (PoS) and PureChain (PoA^2) networks; Section IV-E discusses the human-like feedback for users and Section IV-G concludes with the study limitation. Comparative experiments against baseline models highlight the robustness, efficiency, and dual-task adaptability of RemoteCare in real-time operational scenarios.

A. Proposed RemoteCare Model for Distress Prediction Performance

The experimental evaluations in Table IV demonstrate that the proposed *RemoteCare* framework achieved near-perfect health classification performance, attaining *99.7% accuracy*, *1.00 precision*, *0.994 recall*, and *1.00 F1-score* for acute distress detection. Clinically, these metrics demonstrate highly reliable early-warning capability. The alarm subsystem produced zero missed alarms and a FAR of 0.000.

Reliability Across Folds: To further assess robustness, we repeated training and evaluation using fivefold cross-validation. Results were highly consistent, with standard deviations below 0.3% across accuracy and $F1$-scores. Specifically, health classification achieved 99.7% $\pm$ 0.2% accuracy and 1.00 $\pm$ 0.1 precision, while intrusion detection reached 96.0% $\pm$ 0.3% accuracy and 0.98 $\pm$ 0.2 $F1$-score, demonstrating stable generalization across splits.

Edge Inference Efficiency: This combination ensures timely and accurate triage across diverse acute conditions, including respiratory, cardiovascular, infectious, and metabolic events. In addition to predictive reliability, the system demonstrated a fast inference time of 80 μs per window and a compact model size of 0.45 MB (see Table IV), confirming that *RemoteCare* is lightweight and efficient for real-time, on-device monitoring in resource-constrained IoMT environments. These results establish *RemoteCare* as both clinically dependable and technically optimized for continuous remote patient monitoring.

1) Comparative Evaluation of the Distress Prediction Performance With the Baseline Models: To benchmark the effectiveness of the proposed *RemoteCare* pipeline, we conducted extensive comparative experiments against multiple machine learning and deep learning architectures, including RF, CNN–LSTM, LSTM, SVM, RF–CNN–GRU–LSTM, and CNN models (see Table V). All models were trained and tested on the same preprocessed dataset under identical experimental conditions. For the health classification task, CNN–LSTM and RF–CNN–GRU–LSTM led the baselines with an accuracy of 98.0% and an $F1$-score of 0.98, closely followed by LSTM, also with an $F1$-score of 0.98. The proposed *RemoteCare* model delivered nearly perfect results, attaining 99.7% accuracy, 1.00 precision, 0.994 recall, and 1.00 $F1$-score for the Critical class. This demonstrates the model's exceptional reliability in distinguishing between normal, warning, and critical health states, which is crucial for real-time acute distress monitoring.

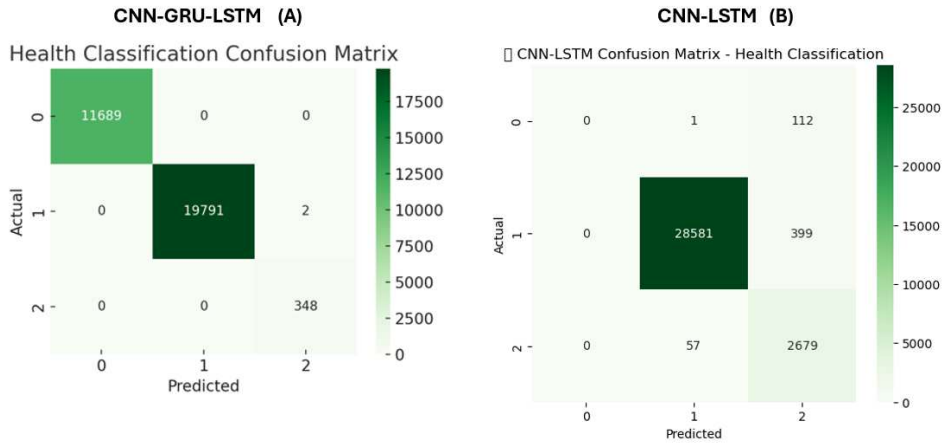

Fig. 3. RemoteCare health classification confusion matrix (left). CNN–LSTM attack detection confusion matrix (right).

Fig. 3(a) shows the confusion matrix for RemoteCare's three-class health classification branch. The class-wise results reveal the following.

1) *Normal (Class 0):* 11 689 correct classifications.
2) *Warning (Class 1):* 19 791 correct, two misclassified as Critical.
3) *Critical (Class 2):* 348 correct classifications.
4) No misclassifications between normal and warning/critical.

Thus,

$$\text{Overall Accuracy} = \frac{11\,689 + 19\,791 + 348}{11\,689 + 19\,791 + 2 + 348} \approx 0.997$$

$$\text{Sensitivity(Critical)} = \frac{348}{348 + 2} \approx 0.994$$

indicates a high prediction accuracy (99.7%) and sensitivity (99.7%) by the proposed *RemoteCare* at any given instance in determining the distress experienced and health status of a patient in real-time.

2) Comparison With CNN–LSTM Baseline: Since CNN–LSTM was the strongest baseline among the tested models, its performance was directly compared to *RemoteCare*. Fig. 3(b) presents the CNN–LSTM confusion matrices for health classification. For *health classification*, *RemoteCare* delivers near-perfect discrimination between normal, warning, and critical categories, with minimal cross-class errors and exceptional accuracy in detecting rare critical cases. In contrast, CNN–LSTM exhibits higher misclassification rates, including notable confusion between Normal and Critical states. These results underscore *RemoteCare*'s superior precision, robustness, and dependability in integrated IoMT security and physiological monitoring (see Fig. 3).

B. Alarm System Metrics and Comparison With the Baseline Models

The health classification output feeds into an alarm system that activates when a *Critical (Class 2)* status is predicted. The system tracks the following.

(i) *True Distress Windows:* Correctly predicted critical states.
(ii) *False Alarms:* Incorrect critical predictions.
(iii) *Missed Distress:* Instances where a true distress state was not predicted.

Table V presents *RemoteCare* alarm system metrics, while the performance metrics for the alarm system for all baseline models, which include FAR, miss rate, sensitivity (TPR), and precision (PPV) compared to *RemoteCare*, were presented in Table VI. These results confirm that the *RemoteCare* pipeline provides highly reliable health distress alerts, virtually eliminating missed events and false alarms, and surpassing the performance reported in comparable literature (see Table VII). Notably, *RemoteCare* achieved *zero missed alarms*, an extremely low false alarm count (8), and the lowest possible FAR and miss rate (both 0.000). Its sensitivity reached 1.000 and precision 0.977, while also maintaining the fastest inference speed (0.000080 s) and smallest model footprint (0.45 MB) among all evaluated deep models. In contrast, competing methods such as CNN–LSTM and LSTM produced more false alarms and higher miss rates, while SVM underperformed in both accuracy and efficiency. Random forest, though highly accurate for attack detection, exhibited substantial model size and a high false alarm burden, limiting its practicality for real-time IoMT deployment.

Equally important, the negligible FAR directly addresses the problem of *alarm fatigue*, a major concern in remote monitoring environments where caregivers may become desensitized to frequent, unreliable alerts. By minimizing false positives, *RemoteCare* ensures that alerts remain clinically meaningful and actionable, thereby preserving trust in the system while reducing unnecessary interventions. Together, these findings establish *RemoteCare* as both clinically dependable and computationally efficient for continuous, real-time patient monitoring.

1) Alarm System and Case Study: The graph for acute health distress events, Fig. 4, illustrates a representative alarm trigger event from the *RemoteCare* health monitoring system at sample index 122. The health class remains stable in either *Normal* or *Warning* states before the acute health

TABLE VI
ALARM PERFORMANCE AND INFERENCE EFFICIENCY OF BASELINE MODELS VERSUS REMOTECARE

Model	False Alarms	MD	FAR	Miss Rate	Sensitivity	Precision	Ave. Inf. Time (s)	Model Size (MB)
Random Forest	2397	204	0.090	0.038	0.962	0.682	0.000017	19.53
CNN-LSTM	764	40	0.026	0.012	0.988	0.764	0.000053	0.45
LSTM	795	135	0.025	0.050	0.950	0.764	0.065206	0.27
SVM	835	1042	0.028	0.419	0.581	0.633	0.001608	1.33
RF-CNN-GRU-LSTM	729	25	0.025	0.010	0.990	0.772	0.000374	0.5
CNN	792	90	0.027	0.036	0.964	0.751	0.000045	0.47
RemoteCare	8.000	0.000	0.000	0.000	1.000	0.977	0.000080	0.45

MD = Missed Detection; FAR = False Alarm Rate; Ave.Inf. = Average Inference

TABLE VII
ALARM PERFORMANCE AND INFERENCE EFFICIENCY OF STATE-OF-THE-ART MODELS

Author	False Alarms	MD	FAR	Miss Rate	Sensitivity	Precision	Ave. Inf. Time (s)	Model Size (MB)
[7]	*	*	*	*	*	*	*	*
[22]	*	*	*	*	*	*	*	*
[8]	29	*	*	*	*	*	0.30	*
[6]	2	3	4	6	94.0	95.9	*	*
RemoteCare	8	0	0.000	0.000	1.000	0.977	0.000080	0.45

* = Not Mentioned; MD = Missed Detection; FAR = False Alarm Rate; Ave.Inf. = Average Inference

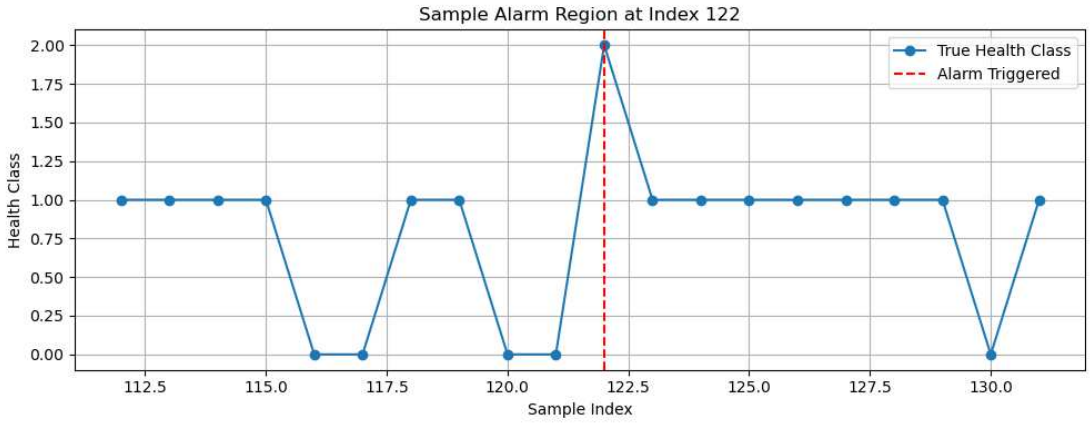

Fig. 4. Alarm system showing true health classes (blue dots) and alarm trigger (red dashed line) at the onset of a distress event. The model's alarm is immediate and accurate.

distress event, before a sudden spike to the *Critical* class (coded as 2) prompts an immediate alarm, indicated by the red dashed vertical line. Following the alarm, the system returns to a noncritical state without spurious retriggering. This demonstrates the framework's ability to detect abrupt critical health changes in real time while avoiding false alarms in preceding windows, thereby ensuring both timely response and operational reliability.

C. Network Attack Resilience Analysis of System

The model attack detection module was evaluated to assess its capability to accurately differentiate between benign and malicious network traffic within the *RemoteCare* framework. By combining convolutional layers for local feature extraction with GRU and LSTM units for short- and long-term temporal dependence modeling, the architecture is designed to capture both abrupt anomalies and evolving intrusion patterns in IoMT network streams. The *RemoteCare* attack detection branch consistently outperformed baseline and most state-of-the-art models, achieving *96.0% accuracy*, *0.96 precision*, *0.99 recall*, and *0.98 F1-score* for binary intrusion detection. Comparative results, Table VIII, show that *RemoteCare* not only competes with but outperforms IDSs, while uniquely combining attack detection and health monitoring in one unified pipeline, capabilities that earlier works typically addressed in isolation.

TABLE VIII
ATTACK DETECTION PERFORMANCE OF BASELINE MODELS

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	0.924	0.94	0.88	0.95
CNN-LSTM	0.929	0.93	0.93	0.93
LSTM	0.911	0.92	0.91	0.92
SVM	0.814	0.83	0.81	0.78
RF-CNN-GRU-LSTM	0.924	0.93	0.92	0.92
CNN	0.850	0.86	0.85	0.83
RemoteCare	0.960	0.96	0.99	0.98

1) Comparative Evaluation of the Network Attack Resilience Performance With the Baseline Models: For the attack detection task, RF and CNN–LSTM achieved

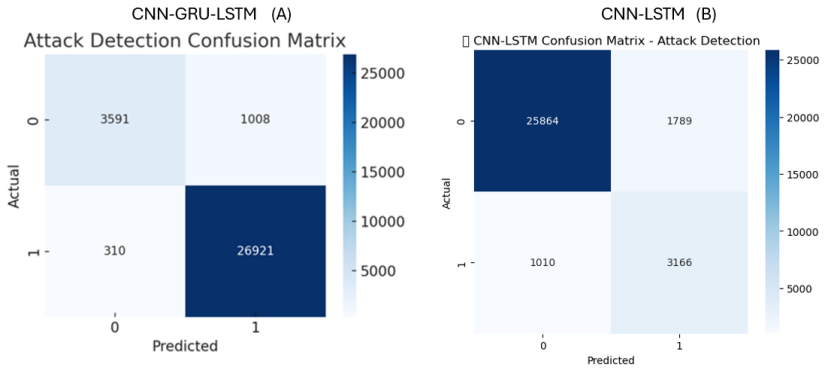

Fig. 5. *RemoteCare* attack detection confusion matrix (left). CNN–LSTM attack detection confusion matrix (right).

Fig. 6. Threat analysis of the `PredictionLogger` smart contract using solidityscan.

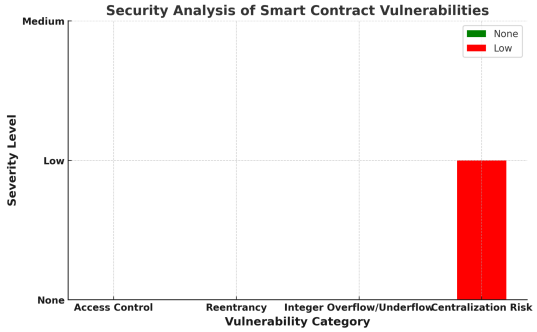

Fig. 7. Security analysis summary of the smart contract.

accuracies of 92.4% and 92.9% with $F1$-scores of 0.95 and 0.93, respectively. The LSTM and RF–CNN–GRU–LSTM baseline yielded an $F1$-score of 0.92. In contrast, the proposed *RemoteCare* model outperformed all baselines, achieving 96.0% accuracy, 0.96 precision, 0.99 recall, and 0.98 $F1$-score. These results in Tables VIII demonstrate *RemoteCare*'s superior capability to detect cyberattacks accurately while minimizing false positives and false negatives.

2) RemoteCare Attack Classification Performance Confusion Metrics: The classification performance of *RemoteCare* was evaluated for *attack detection*, using confusion matrices and standard evaluation metrics. Fig. 5(a) presents the confusion matrix for *RemoteCare*'s attack detection branch.

Thus,

$$\text{Accuracy} = \frac{26921 + 3591}{26921 + 3591 + 1008 + 310} \approx 0.960$$

$$\text{Precision} = \frac{26921}{26921 + 1008} \approx 0.964$$

$$\text{Recall(Sensitivity)} = \frac{26921}{26921 + 310} \approx 0.989$$

$$F1 \text{ Score} \approx 0.976$$

indicating that the *REmoteCare* achieved a highly accurate and precise network attack prediction with dynamic change in the behavior of data transmission characteristics from the edge devices in the IoMT. Furthermore, *RemoteCare* achieves a more favorable precision–recall balance by reducing false positives from 1789 (CNN–LSTM) to 1008 while keeping false negatives low, resulting in more accurate detection of both normal and malicious traffic.

D. PureChain Metrics and Security Analysis

The *PureChain*-based *PredictionLogger* smart contract, combined with IPFS for scalable off-chain storage, enables *tamper-proof, low-latency, and zero-cost logging* of predictions. The results in Table IX demonstrate that PureChain's *PoA*^{2} consensus achieves significantly lower latency (0.2572 s) and higher throughput (69.03 TPS) compared to Ethereum's PoS, enabling high-frequency on-chain updates without economic or performance bottlenecks. Two different threat analyses were conducted to show the security resilience of our smart contract. Figs. 6 and 7 show the threat analysis report of the `PredictionLogger` contract, which was assessed as *Low Risk (97/100)* with no high- or moderate-severity issues. This independent audit reinforces that the blockchain component is secure under adversarial conditions such as reentrancy, unauthorized access, or transaction replay.

On-Chain Logging Throughput and Real-Time Suitability: Although block confirmation introduces latency, the PureChain network uses PoA^2 consensus to sustain high throughput suitable for IoMT streams. In our measurements, see Section IV-D, PureChain mean latency and TPS substantially outperform Ethereum PoS latency and TPS. To avoid backpressure during transient bursts, the gateway (see Algorithm 2) optionally offloads full payloads to IPFS and logs compact byte summaries (or CIDs) on-chain, pre-

TABLE IX
PERFORMANCE COMPARISON BETWEEN ETHEREUM AND PURECHAIN NETWORK

Metric	Ethereum Mainnet	PureChain (Zero-Fee)
Latency (Mean) s	6.572	0.2572
TPS (Mean)	15.21	69.03
Gas Cost per Tx	$0.41–$1.50+	$0 (Free)
Consensus Algorithm	PoS)	PoA^2)

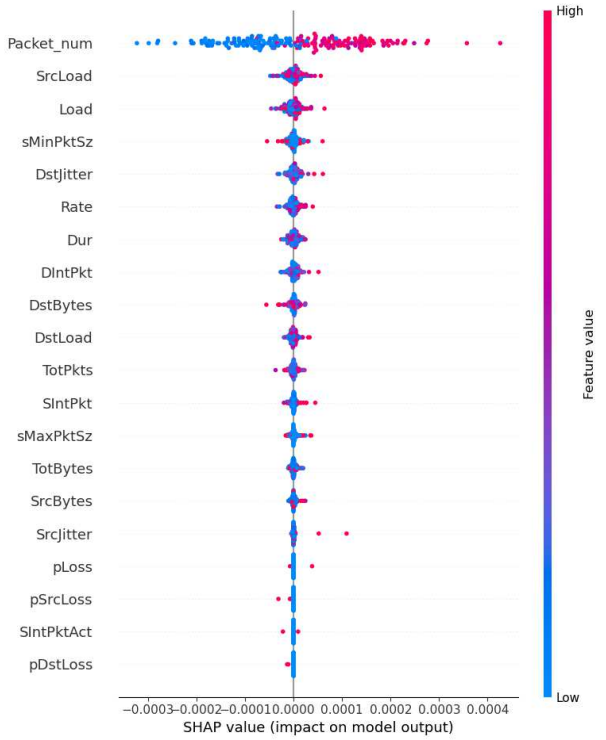

Fig. 8. SHAP summary plot. Top network features impacting attack prediction. Features with higher absolute SHAP values have greater influence on the model output.

serving real-time behavior while maintaining tamper-evident auditability.

E. Interpretable End-User Feedback

The XAI is satisfied through SHAP-based analysis, which identified dominant network features (such as *Packet_num*, *Load*, and *DIntPkt*) and physiological drivers (such as *Heart_rate*, *Resp_Rate*, and *SpO$_2$*) influencing predictions. These interpretable visualizations enhance transparency, enabling clinicians and operators to understand and trust model outputs. The results confirm that *RemoteCare* not only meets its design objectives, delivering a high-performance, explainable solution for a simultaneous health state classification and intrusion mitigation in IoMT environments.

Figs. 8 and 9 illustrate the SHAP summary plots for attack (network) and health (physiological) features, respectively. These plots demonstrate that the model's attack prediction is primarily influenced by traffic-related features, such as `Packet_num`, `Load`, `SrcLoad`, and `DIntPkt`, while health predictions rely on `Heart_rate`, `Resp_Rate`, and `SpO2`. The color mapping reveals how high or low values of

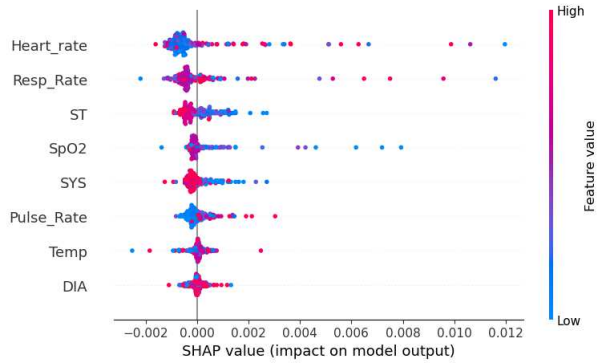

Fig. 9. SHAP summary plot. Physiological features contributing to health status prediction. Key drivers include `Heart_rate`, `Resp_Rate`, and `SpO2`.

TABLE X
HEALTH CLASSIFICATION PERFORMANCE OF STATE-OF-THE-ART MODELS

Author	Model	Acc.	Prec.	Rec.	F1
[31]	CNN	90.00	90.00	95.00	92.00
[32]	SVM	94.20	93.50	95.00	94.20
[33]	LSTM	92.30	–	–	–
RemoteCare	CNN–GRU–LSTM	99.70	100.00	99.40	100.00

each feature shift the model output. This level of transparency allows domain experts to verify model behavior and builds trust in critical healthcare applications.

Overall, *RemoteCare* achieved 99.7% accuracy for health classification and 96.0% for intrusion detection, with low FARs and efficient inference times, demonstrating robustness in real-time monitoring. Beyond raw accuracy, *personalization improved clinical reliability*. By aligning thresholds to patient-specific baselines, *RemoteCare* reduced false alarms that typically arise when population norms are applied universally. This adaptive monitoring is particularly valuable for patients with chronic conditions (e.g., COPD, hypertension, or arrhythmia), where deviations from an individual's own baseline are more predictive of deterioration than deviations from generic reference ranges. Moreover, the incorporation of SHAP-based interpretability provided *clinician-oriented insights*, enabling healthcare providers to understand which physiological parameters or network factors most influenced each prediction. In doing so, *RemoteCare* bridges the gap between algorithmic output and medical reasoning, thereby enhancing trust, usability, and clinical decision support in real-world remote monitoring scenarios.

F. Performance Evaluation With Related Works

1) RemoteCare Health Classification Performance Versus State-of-the-Art Models: Table X compares the health classification performance of *RemoteCare* against previous works that considered physiological status prediction. While models such as CNN [31] and SVM [32] demonstrated solid results, they were constrained to the health monitoring domain and lacked integrated intrusion detection capability. The *RemoteCare* framework achieved *99.7% accuracy*, *100% precision*, *99.4% recall*, and *100% F1-score* for critical health status

TABLE XI
ATTACK DETECTION PERFORMANCE OF STATE-OF-THE-ART MODELS

Author	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
[7]	CNN	85.00	93.00	85.00	88.00
[7]	SVM	100.00	100.00	100.00	100.00
[22]	DQN	92.40	–	–	–
[6]	RF	95.00	94.00	–	–
[8]	RF	94.50	–	–	–
[12]	Ensemble (DT/RF/XGB/ET/GB)	99.44	99.76	99.45	99.61
[17]	XGB	92.60	92.80	92.60	92.60
Ours	CNN–GRU–LSTM	96.00	96.00	99.00	98.00

detection, outperforming all referenced works and providing a unified solution that merges high-accuracy health monitoring with robust cyberattack detection.

The *RemoteCare* health classification surpassed the best existing results [31], [32] by achieving perfect precision and near-perfect recall, ensuring reliable detection of critical cases with minimal false alarms. Its dual-domain superiority validates *RemoteCare* as a practical, high-performance framework for integrated IoMT security and physiological monitoring, bridging a gap unaddressed by prior single-focus approaches.

2) RemoteCare Attack Detection Performance Versus State-of-the-Art Models: Table XI presents the benchmarking of the proposed *RemoteCare* model against state-of-the-art machine learning and deep learning approaches for network intrusion detection. While several prior works, such as SVM [7] and ensemble tree-based models [12], achieved high accuracy (with SVM reaching perfect scores), these models were evaluated exclusively for attack detection and lacked any capability for health status monitoring. The *RemoteCare* model, based on a hybrid CNN–GRU–LSTM architecture, achieved competitive results with *96.0% accuracy*, *96.0% precision*, *99.0% recall*, and *98.0% F1-score*, placing it among the top performers while also supporting multidomain functionality absent in prior work. The *RemoteCare* attack detection achieved a recall improvement of up to 14% over traditional CNN architectures [7] and delivered competitive precision relative to the top ensemble model [12].

G. Significance and Limitations of Study

The proposed *RemoteCare* framework demonstrates the effectiveness of integrating CNNs, GRUs, and LSTM networks in a hybrid architecture for real-time health status monitoring and cyberattack detection within IoMT environments. By fusing these heterogeneous feature representations and leveraging a dual-output classification strategy, *RemoteCare* achieves high accuracy for both binary attack detection and multiclass health state classification. This dual detection capability is crucial in mission-critical settings, such as military healthcare and remote patient monitoring, where timely and accurate alerts can significantly improve intervention outcomes. Furthermore, the on-chain logging of predictions enhances system transparency, auditability, and trustworthiness.

A key strength of *RemoteCare* lies in its ability to deliver *personalized monitoring* that adapts to individual patient profiles. Consider, for instance, a COPD patient whose baseline oxygen saturation (SpO_2) is consistently lower than the population norm. Conventional threshold-based monitoring systems would frequently misclassify this patient as being in a critical state, leading to unnecessary alarms and potential alarm fatigue. In contrast, *RemoteCare* recalibrates its thresholds relative to the patient's own baseline, ensuring that only clinically meaningful deviations trigger alerts. Similarly, a hypertensive patient with naturally elevated systolic blood pressure is monitored against their personal reference range, improving both sensitivity and specificity. The SHAP-based interpretability layer further enhances this personalization by revealing to clinicians why a particular decision was made for that patient at that time, such as highlighting the combined influence of declining SpO_2 and an elevated respiratory rate. This synergy between adaptive thresholds and explainable outputs not only reduces false positives but also strengthens clinician trust, paving the way for practical deployment in telehealth and remote care ecosystems.

Despite the strong performance exhibited by *RemoteCare*, the model was trained and evaluated on the WUSTL-EHMS-2020 dataset, which, while comprehensive, may not encompass all real-world IoMT deployment conditions, including extreme environmental noise and device heterogeneity. This limitation may affect the robustness of *RemoteCare* in detecting other types of cyberattacks in IoMT and vital signs, which are not covered in the WUSTL-EHMS-2020 dataset.

V. CONCLUSION

This article presented *RemoteCare*, an AI-driven multimodal framework for personalized remote healthcare in IoMT environments. By fusing physiological and network data streams through a hybrid CNN–GRU–LSTM model, *RemoteCare* simultaneously performs health state classification and cyberattack detection, achieving 99.7% and 96.0% accuracy, respectively, on the WUSTL-EHMS-2020 dataset. Beyond raw performance, the framework introduces personalization by dynamically aligning thresholds to individual patient baselines. This reduces false alarms and improves the clinical reliability of predictions. This adaptive monitoring is particularly valuable for chronic conditions, such as COPD, hypertension, or arrhythmia, where deviations from personal norms are more predictive of deterioration than generic population thresholds.

In addition, the SHAP-based interpretability layer provides clinician-oriented insights, highlighting patient-specific drivers of predictions and bridging the gap between algorithmic out-

put and medical reasoning. Immutable blockchain and IPFS logging ensure secure, auditable, and patient-controlled monitoring records, further enhancing trust. Overall, *RemoteCare* advances remote patient monitoring by integrating personalization, interpretability, and cybersecurity into a unified pipeline. The limitations of this work remain the evaluation on a single dataset, which may not capture the diversity of attack patterns and physiological conditions encountered in real-world deployments. Future work will validate the framework in clinical trials, extend personalization to diverse cohorts, and use multisource datasets such as ToN-IoT, which include richer cyberattack scenarios and heterogeneous IoMT environments, and integrate RemoteCare into telehealth platforms for scalable and patient-centered healthcare delivery.

Conflict of 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 article.

References

[1] O. I. Obaid and S. A.-B. Salman, "Security and privacy in IoT-based healthcare systems: A review," *Mesopotamian J. Comput. Sci.*, vol. 2022, pp. 29–39, Dec. 2022.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[3] F. Imrie, S. Denner, L. S. Brunschwig, K. Maier-Hein, and M. van der Schaar, "Automated ensemble multimodal machine learning for healthcare," *IEEE J. Biomed. Health Informat.*, vol. 29, no. 6, pp. 4213–4226, Jun. 2025.

[4] A. Chaudhary, V. Khullar, and K. Kaushik, "Guest editorial: Advancing personalized healthcare integrating AI and health informatics," *IEEE J. Biomed. Health Informat.*, vol. 29, no. 7, pp. 4597–4598, Jul. 2025.

[5] P. Jayant, E. Vincent, Mohana, M. Moharir, and A. R. A. Kumar, "Smart health monitoring and anomaly detection using Internet of Things (IoT) and artificial intelligence (AI)," in *Proc. 2nd Int. Conf. Intell. Cyber Phys. Syst. Internet Things (ICoICI)*, Aug. 2024, pp. 479–485.

[6] G. X. Wong, H. Tung Yew, J. A. Diargham, F. Wong, M. Mamat, and S. K. Chung, "IoMT real-time health monitoring system," in *Proc. 12th Int. Conf. Awareness Sci. Technol. (iCAST)*, Nov. 2023, pp. 269–273.

[7] O. P. Olawale and S. Ebadinezhad, "Cybersecurity anomaly detection: AI and Ethereum blockchain for a secure and tamperproof IoHT data management," *IEEE Access*, vol. 12, pp. 131605–131620, 2024.

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

[9] T. Shaik, X. Tao, L. Li, H. Xie, and J. D. Velásquez, "A survey of multimodal information fusion for smart healthcare: Mapping the journey from data to wisdom," *Inf. Fusion*, vol. 102, Feb. 2024, Art. no. 102040. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253523003561

[10] S. Kayalvizhi, S. Nagarajan, J. Deepa, and K. Hemapriya, "Multimodal IoT-based medical data processing for disease diagnosis using heuristic-derived deep learning," *Biomed. Signal Process. Control*, vol. 85, Aug. 2023, Art. no. 104889. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1746809423003221

[11] D. Schouten et al., "Navigating the landscape of multimodal AI in medicine: A scoping review on technical challenges and clinical applications," *Med. Image Anal.*, vol. 105, Oct. 2025, Art. no. 103621. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361841525001689

[12] K. Gupta, K. D. Gupta, D. Kumar, G. Srivastava, and D. K. Sharma, "BIDS: Blockchain and intrusion detection system coalition for securing Internet of Medical Things networks," *IEEE J. Biomed. Health Informat.*, early access, Oct. 19, 2024, doi: 10.1109/JBHI.2023.3325964.

[13] S. O. Ajakwe, K. L. Olabisi, and D.-S. Kim, "Multihop intruder node detection scheme (MINDS) for secured drones' FANET communication," *IET Intell. Transp. Syst.*, vol. 19, no. 1, p. 70080, Jan. 2025.

[14] V. Ravi, T. D. Pham, and M. Alazab, "Deep learning-based network intrusion detection system for Internet of Medical Things," *IEEE Internet Things Mag.*, vol. 6, no. 2, pp. 50–54, Jun. 2023.

[15] H. Goumidi and S. Pierre, "Real-time anomaly detection in IoMT networks using stacking model and a healthcare-specific dataset," *IEEE Access*, vol. 13, pp. 70352–70365, 2025.

[16] M. Benmalek, A. Seddiki, and K.-D. Haouam, "SNN-IoMT: A novel AI-driven model for intrusion detection in Internet of Medical Things," *Comput. Model. Eng. Sci.*, vol. 143, no. 1, pp. 1157–1184, 2025.

[17] M. M. Alani, A. Mashatan, and A. Miri, "Explainable ensemble-based detection of cyber attacks on Internet of Medical Things," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Nov. 2023, pp. 609–614.

[18] R. Kalakoti, S. Nõmm, and H. Bahsi, "Explainable transformer-based intrusion detection in Internet of Medical Things (IoMT) networks," in *Proc. Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2024, pp. 1164–1169.

[19] F. Binsar, "Trustworthy and interpretable AI in IoT-based medical systems: A review and framework for COT-XAI integration," *J. Intell. Syst. Internet Things*, vol. 18, pp. 169–184, Jul. 2025.

[20] A. Aljuhani, "IDS-chain: A collaborative intrusion detection framework empowered blockchain for Internet of Medical Things," in *Proc. IEEE Cloud Summit*, Oct. 2022, pp. 57–62.

[21] A. K. Tyagi, T. T. George, and G. Soni, "Blockchain-based cybersecurity in internet of medical things (IoMT)-based assistive systems," in *AI-Based Digital Health Communication for Securing Assistive Systems*. IGI Global, Oct. 2023, pp. 22–53.

[22] L. A. Daher, "Towards secure IoMT: Attack detection using deep Q-learning in healthcare networks," in *Proc. 16th Int. Conf. Develop. eSystems Eng. (DeSE)*, Dec. 2023, pp. 407–412.

[23] N. C. Kavkas and K. Yildiz, "Enhancing IoMT security with deep learning based approach for medical IoT threat detection," in *Proc. 13th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Apr. 2025, pp. 1–5.

[24] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1969–1976, May 2022.

[25] F. E. Shamout, T. Zhu, P. Sharma, P. J. Watkinson, and D. A. Clifton, "Deep interpretable early warning system for the detection of clinical deterioration," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 2, pp. 437–446, Feb. 2020.

[26] S. Sung, Y. S. Bae, Y. Kim, J. Woo, and E. K. Chie, "Development of remote patient monitoring system for patients with COVID-19 infection based on the predictive algorithms," in *Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM)*, Dec. 2023, pp. 4955–4956.

[27] B. Zaabar, O. Cheikhrouhou, and M. Abid, "Intrusion detection system for IoMT through blockchain-based federated learning," in *Proc. 15th Int. Conf. Secur. Inf. Netw. (SIN)*, Nov. 2022, pp. 01–08.

[28] G. B. Smith, D. R. Prytherch, P. Meredith, P. E. Schmidt, and P. I. Featherstone, "The ability of the national early warning score (news) to discriminate patients at risk of early cardiac arrest, unanticipated intensive care unit admission, and death," Centre Postgraduate Med. Res. Educ. (CoPMRE), School Health Social Care, Bournemouth Univ., Bournemouth, U.K., 2013. [Online]. Available: https://eprints.bournemouth.ac.uk/25324/26/Smith.%20NEWS.pdf

[29] C. A. Nnadiekwe, V. I. Kalu, G. C. Akor, and D.-S. Kim, "Blockchain-enabled lightweight data management in smart factories," in *Proc. Korea Inst. Commun. Inf. Sci.*, 2025, pp. 567–568. [Online]. Available: https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE12132120

[30] I. S. Igboanusi, R. N. Alief, M. R. R. Ansori, J.-M. Lee, and D.-S. Kim, "Ethereum based storage aware mining for permissioned blockchain network," in *Proc. 13th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2022, pp. 161–166.

[31] H. Lu, X. Feng, and J. Zhang, "Early detection of cardiorespiratory complications and training monitoring using wearable ECG sensors and CNN," *BMC Med. Informat. Decis. Making*, vol. 24, no. 1, pp. 194–215, Jul. 2024.

[32] J. Zhang, "Health monitoring and safety early warning system for foundation pit support structure using support vector machine and ensemble learning algorithm," in *Proc. IEEE Int. Conf. Electron., Energy Syst. Power Eng. (EESPE)*, Mar. 2025, pp. 1270–1274.

[33] P. Chen and J. Li, "Construction of a physical health monitoring platform for adolescents driven by big data," in *Proc. 4th Int. Conf. Inf. Technol. Contemp. Sports (TCS)*, Dec. 2024, pp. 120–123.

Chigozie Athanasius Nnadiekwe received the B.Tech. and M.Sc. degrees in biomedical engineering from the Federal University of Technology, Owerri, Nigeria, in 2014 and 2021, respectively. He is currently pursuing the Ph.D. degree with IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea.

He serves as a Lecturer with the Department of Biomedical Engineering, David Umahi Federal University of Health Sciences, Uburu, Nigeria. He is the Lead Developer of the RemoteCare framework, which integrates AI-driven physiological analytics with secure blockchain logging to enable trustworthy, explainable health monitoring in distributed Internet of Medical Things (IoMT) environments. His research focuses on blockchain-assisted IoMT systems, secure medical data management, and hybrid deep learning models for real-time health and cyberattack detection.

Simeon Okechukwu Ajakwe (Senior Member, IEEE) received the Diploma degree in computer science from Imo State University, Owerri, Nigeria, in 2004, the B.Sc. degree from the Institute of Management Technology, Enugu, Nigeria, in 2009, the M.Sc. degree (Hons.) in information technology from the Federal University of Technology, Owerri, Imo, in 2016, and the Ph.D. degree (Hons.) from the IT-Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea, in 2023.

He is a Chartered Information Technology Professional (Citp) with many years of IT-related industrial and academic experience. He is a Post-Doctoral Research Fellow with the ICT Convergence Research Center (ICT-CRC), Kumoh National Institute of Technology. He has authored or co-authored several articles and conference papers. His research interests include artificial intelligence (AI) for aerial mobility, trustworthy AI, network security, deep learning and computer vision, and information system security.

Dr. Ajakwe is a member of the Association of Computing Machinery (ACM), the Computer Professionals of Nigeria (CPN), and Nigerian Internet Society (NIS). He has received several awards, such as the Best Ph.D. Thesis Award, the Best Paper Award, and the Research Excellence Award. He has served as an Editor, a Guest Editor, and a reviewer for reputable peer-reviewed journals.

Jae-Min Lee (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2005.

From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2015 to 2016, he was a Principal Engineer with Samsung Electronics. Since 2017, he has been an Assistant Professor with the School of Electronic Engineering and the Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongbuk, South Korea. His current main research interests are industrial wireless control networks, performance analysis of wireless networks, and TRIZ.

Dong-Seong Kim (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003.

From 1994 to 2003, he worked as a Full-Time Researcher with ERCACI, Seoul National University. From March 2003 to February 2005, he worked as a Post-Doctoral Researcher with the Wireless Network Laboratory, School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor with the Department of Computer Science, University of California at Davis, Davis, CA, USA. He is currently the Director of KIT Convergence Research Institute and ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program) supported by Korean Government with Kumoh National Institute of Technology, Gumi, South Korea. His current main research interests are real-time IoT and smart platforms, industrial wireless control networks, networked embedded systems, and fieldbus.

Prof. Kim is a Senior Member of ACM.