RemoteCare: Secure and Explainable Dual-Task Health and Cyberattack Detection Framework for IoMT

Chigozie Athanasius Nnadiekwe[1], Simeon Okechukwu Ajakwe[2], Jae Min Lee[1], Dong-Seong Kim[1*]
[1] IT-Convergence Engineering Department, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT-Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
*NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea

***Abstract*—The Internet of Medical Things (IoMT) enables continuous physiological monitoring but remains vulnerable to cyberattacks and opaque decision-making. This paper presents RemoteCare, a secure and explainable dual-task framework for real-time health and attack detection. RemoteCare employs a hybrid CNN–GRU–LSTM architecture to jointly classify physiological states (Normal, Warning, Critical) and detect network intrusions, with SHAP-based interpretability ensuring transparent predictions. Predictions are immutably logged on the PureChain blockchain and linked to IPFS for scalable storage. Experiments on the WUSTL-EHMS-2020 dataset demonstrate 99.7% health classification accuracy and 96.0% attack detection accuracy, outperforming state-of-the-art baselines. Benchmarking further shows PureChain achieves 0.2572 s latency and zero-cost transactions, validating RemoteCare as a reliable, auditable IoMT monitoring solution.**

***Index Terms*—IoMT, Cyberattack Detection, Real-Time Monitoring, XAI, Multimodal Data Fusion, Blockchain-Based Prediction Logging.**

I. INTRODUCTION

The IoMT has rapidly evolved from simple sensor-based monitoring into a transformative ecosystem of interconnected devices enabling continuous, real-time healthcare delivery. Its most prevalent applications include patient vital-sign tracking and chronic disease management; however, IoMT is increasingly being deployed in mission-critical domains such as military healthcare, battlefield casualty monitoring, and disaster response coordination [1]. These environments demand rapid, data-driven decisions where delays can significantly impact morbidity and mortality outcomes. Through wearable devices and edge/cloud platforms, IoMT enables the continuous monitoring of key physiological signals such as heart rate, SpO_2, respiratory rate, and blood pressure [2]. This capability is particularly critical in remote or high-risk settings, where access to traditional medical infrastructure is limited. Moreover, by integrating IoMT with artificial intelligence (AI) and blockchain technologies, healthcare systems are shifting from reactive to proactive care paradigms [3]. These integrations enhance system resilience, ensure data transparency, and foster trust in patient monitoring workflows, ultimately improving health outcomes across diverse clinical and operational contexts.

Despite this progress, IoMT systems face two critical challenges: (*i*) accurate health state prediction from heterogeneous physiological data and (*ii*) robust defense against cyber threats such as spoofing, denial-of-service, and data tampering [4] etc. Prior works have addressed either health monitoring [1] or intrusion detection independently [5], but very few integrate both domains. Explainable AI (XAI) has been introduced to improve interpretability [6], and blockchain has been explored for secure IDS logging [4], proving to be a veritable tool for privacy preservation in IoMT [7]. However, these approaches remain siloed, often lacking real-time deployment, dual-task capability, or role-based access to sensitive results [8].

In mission-critical IoMT scenarios, concurrent health anomalies and cyberattacks may occur, requiring a unified, explainable, and auditable framework. Existing health monitoring solutions often fail to account for adversarial risks, while IDS methods frequently overlook patient well-being. Moreover, the absence of transparent decision support and immutable audit trails limits clinician trust and system accountability. A holistic approach that fuses multimodal IoMT data, applies XAI across both health and attack predictions, and ensures secure blockchain-backed traceability is therefore necessary to bridge this gap and enhance operational reliability.

To address these challenges, we propose **RemoteCare**, a blockchain-assisted hybrid deep learning framework for real-time health monitoring and cyberattack detection in IoMT. The developed edge-based hybrid deep learning model possesses a dual functional capacity, enabling it to detect the health status of users in real-time and identify cyber-attacks within the network pipeline. On the other hand, the resource-friendly blockchain security framework ensures speedy and energy-efficient tamper-proof validation of access is maintained.

Therefore, the key contributions of this study are:

- A precision-conscious and dual-task CNN–GRU–LSTM architecture for simultaneous physiological state classification and intrusion detection is developed.
- Blockchain-enabled auditability via PureChain and IPFS, offering immutable and role-based access control, is integrated.
- SHAP-based explainability applied to both outputs, ensuring transparent and trustworthy decision support for understandable end-user feedback..

TABLE I
SUMMARY OF REVIEWED WORKS AND LIMITATIONS ADDRESSED

Authors	Dataset	AI Model(s)	Blockchain	XAI	Focus	Key Contributions	Limitations
[4]	TON_IoT, Edge_IIoT, UNSW-NB15	SVM, RF, DT, GB, CNN, LSTM, CNN-LSTM	Yes	No	Attacks	Compared classical ML and DL models for anomaly detection; on-chain/IPFS data security	Slow simulations; blockchain test complexity
[5]	Not stated	Deep Q-Learning +SVM	No	No	Attacks	DRL for attack classification, DDoS emphasis	No blockchain/XAI; no health status
[9]	WUSTL-EHMS 2020	KNN, SVM, RF, etc. (comparative)	No	No	Attack	Built a real-time EHMS testbed combining medical and network features	No blockchain/XAI
[10]	Wearables/vitals + alerts	Thresholding, simple ML	No	No	Health	End-to-end remote monitoring	No IDS/XAI/blockchain
RemoteCare (Ours)	WUSTL-EHMS-2020	Hybrid CNN–GRU–LSTM with SHAP	Yes	Yes	Health + Attack	Dual-task real-time classification + intrusion detection; blockchain + IPFS audit trail	

The rest of the paper is organized as follows: Section II reviews related work; Section III details the methodology; Section IV presents experimental results; and Section V concludes with implications and future directions.

II. RELATED WORKS

As seen in Table I, the work on IoMT anomaly detection and monitoring has produced several noteworthy contributions, but existing work often remains limited in scope compared to the holistic goals of **RemoteCare**. Olawale et al. [4] investigated anomaly detection using classical and deep learning models (SVM, RF, DT, GB, CNN, LSTM, CNN–LSTM) across diverse datasets such as TON_IoT and UNSW-NB15. Their work integrated blockchain and IPFS for tamperproof logging, but evaluations suffered from slow simulations and deployment complexity, with no health monitoring or explainability components.

Daher [5] employed Deep Q-Learning with an SVM baseline for intrusion detection in IoMT healthcare networks, focusing on DDoS attack classification. While effective for adaptive attack detection, the study did not incorporate blockchain for integrity or XAI for interpretability, and it excluded health-related predictions. Similarly, Hady et al. [9] developed a real-time testbed (WUSTL-EHMS-2020) that fused medical and network data to evaluate classical ML methods such as KNN, SVM, and RF. Although this work highlighted the benefit of multi-domain feature integration, it lacked blockchain-based auditability and did not include explainability layers, limiting clinical trust in predictions. In contrast, Wong et al. [10] proposed an IoMT monitoring system based on thresholding and simple machine learning for wearables, focusing solely on patient vitals. Their system provided end-to-end monitoring but did not integrate intrusion detection, blockchain, or interpretability, leaving it vulnerable to cyber threats and limited in transparency.

In summary, while prior works have either explored blockchain-based anomaly detection [4], advanced IDS techniques without health prediction [5], [9], or lightweight health monitoring [10], none provide a unified, real-time framework that addresses both health and security domains. **RemoteCare** distinguishes itself by combining a hybrid CNN–GRU–LSTM architecture for dual-task classification, SHAP-based interpretability for both health and attack predictions, and PureChain blockchain with IPFS for zero-cost, low-latency, tamperproof audit trails, thereby addressing the limitations identified in earlier studies (Table I).

III. SYSTEM DESIGN AND METHODOLOGY

The architecture of **RemoteCare** Fig. 1 is composed of four tightly integrated layers: sensing, AI inference, blockchain/IPFS logging, and explainability feedback. At the *sensing layer*, wearable and IoMT devices capture multimodal data such as heart rate, respiratory rate, and network traffic metrics. This layer ensures **reliability** by providing continuous, real-time data streams. The *AI inference layer* processes these streams through a hybrid CNN–GRU–LSTM model, responsible for both health state prediction and attack detection, thus embedding **intelligence** into the pipeline. The *blockchain/IPFS layer* secures outputs by immutably recording predictions on-chain while storing bulk data in distributed storage, guaranteeing **integrity**. Finally, the *XAI feedback layer* employs SHAP to provide interpretability of both health and attack classifications, enhancing system **transparency** and building trust among clinicians and operators.

RemoteCare employs a hybrid CNN–GRU–LSTM architecture designed to capture both short-term patterns and long-term dependencies in heterogeneous IoMT data. The model is structured into two specialized branches. The *network branch* applies 1D convolutional layers with a kernel size of 1, followed by dense bottlenecks, to emphasize inter-channel correlations across traffic attributes rather than temporal dependencies. This ensures that short bursts in network traffic and abrupt anomalies are effectively captured. The *health branch* integrates a GRU layer for efficient intermediate memory retention, followed by a stacked LSTM layer that models long-term physiological trends. This sequential design balances computational efficiency with the ability to detect both mid-range and slowly evolving health deterioration patterns, such as hypoxia or cardiac distress.

The embeddings from both branches are concatenated, regularized with dropout, and passed into dual-output heads: (i) a sigmoid classifier for binary attack detection and (ii) a softmax

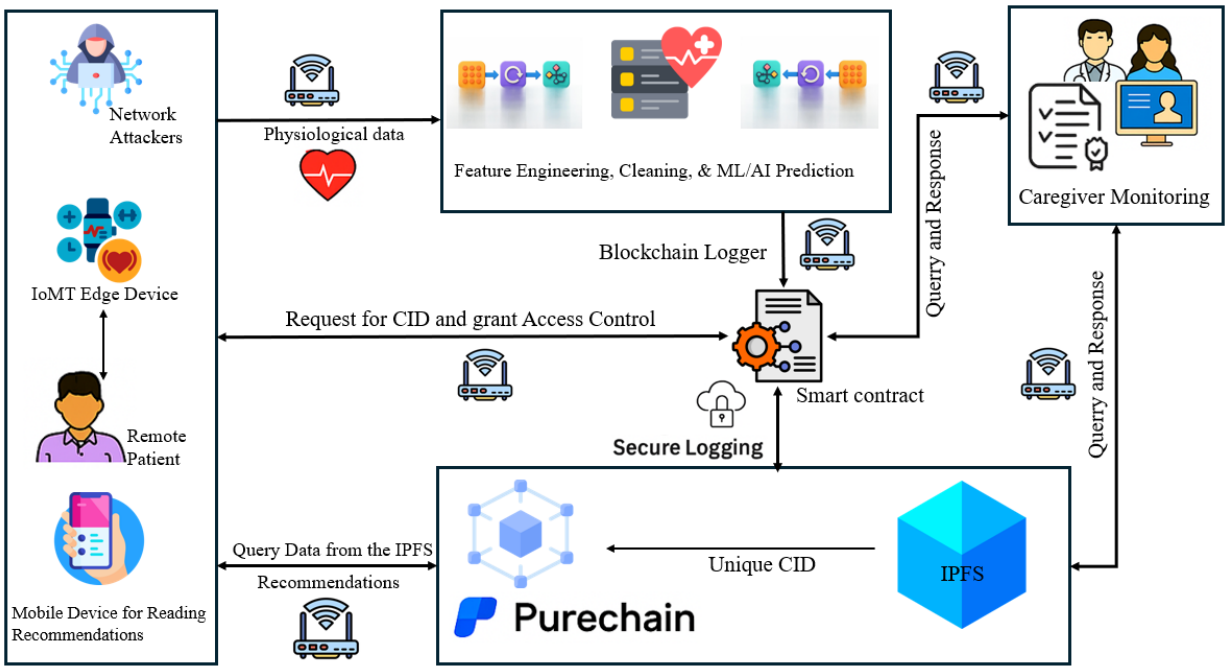

Fig. 1. The proposed System Architecture for RemoteCare

classifier for three-class health state prediction (Normal, Warning, Critical). This multitask learning strategy not only reduces redundancy by sharing learned representations but also acts as a form of regularization, improving generalization across both health and attack prediction tasks. In addition, a rule-based health categorization layer, aligned with the National Early Warning Score (NEWS) clinical guidelines, complements the model by flagging critical anomalies for immediate alarms even before full inference. This hybrid of data-driven learning and clinically validated thresholds ensures rapid intervention in mission-critical scenarios while maintaining the robustness of deep learning predictions.

Let $X^{(n)} \in \mathbb{R}^{T\times F_n}$ denote the network features over a sliding window of length T, and $X^{(h)} \in \mathbb{R}^{T\times F_h}$ denote the synchronized physiological features. The hybrid architecture is designed as follows:

Network Branch (CNN). A 1D convolution with kernel size 1 captures local channel interactions:

$$H_t^{(n)} = \sigma\left(W^{(n)} * X_t^{(n)} + b^{(n)}\right), \tag{1}$$

followed by flattening and dense projection.

Health Branch (GRU–LSTM). Temporal structure in vital signs is modeled by a GRU layer followed by an LSTM for long-term dependencies:

$$h_t = (1-z_t)\odot h_{t-1} + z_t \odot \tilde{h}_t, \quad c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t, \tag{2}$$

where z_t and r_t are GRU update and reset gates, and (i_t, f_t, o_t) are LSTM input, forget, and output gates.

Feature Fusion and Outputs. The learned representations are concatenated:

$$z = \phi\left([z^{(n)}; z^{(h)}]W_f + b_f\right), \tag{3}$$

then mapped to two outputs:

$$\hat{y}^{(a)} = \sigma(W_a z + b_a), \quad \hat{y}^{(h)} = \text{softmax}(W_h z + b_h),$$

where $\hat{y}^{(a)} \in \{0,1\}$ (attack/normal) and $\hat{y}^{(h)} \in \{0,1,2\}$ (Normal, Warning, Critical).

The multi-task objective combines binary cross-entropy for attack detection and categorical cross-entropy for health prediction:

$$\mathcal{L} = \alpha \cdot \text{BCE}(y^{(a)}, \hat{y}^{(a)}) + \beta \cdot \text{CE}(y^{(h)}, \hat{y}^{(h)}), \tag{4}$$

with weights α, β balancing the two tasks.

Blockchain and IPFS Integration: To ensure auditability and tamperproof integrity, all model predictions are logged through a *PredictionLogger* smart contract deployed on the PureChain blockchain. This decentralized framework guarantees both data integrity and auditability while embedding strong security mechanisms [11]. **PureChain** is a specialized blockchain platform designed to overcome the core "quadlemma" challenges of decentralization, security, scalability, and transaction cost efficiency [12]. Its capabilities include zero transaction fees, user-friendly interfaces, an intuitive API, full EVM compatibility, Python-based readability and deployment, robust cryptographic standards, and integrated account management.

Predictions generated by the inference model are securely logged using a blockchain-backed mechanism. The workflow begins with a prediction event, which is encoded into a transaction that includes metadata such as `sender`, `timestamp`, and the hash of the prediction stored in IPFS as a Content Identifier (CID). A simplified transaction format is given below:

```
{
  "sender": 0x1234...ABCD,
  "timestamp": 1695256102,
  "health_class": "Critical",
  "attack_class": "Attack",
  "cid": "QmXYZ...123"
}
```

This transaction is submitted to the smart contract, immutably recorded on-chain, and linked to the corresponding data in IPFS. The contract, built using Solidity and OpenZeppelin's AccessControl, enforces role-based permissions (`LOGGER_ROLE`) so that only authorized devices can submit records. Each log entry contains the sender's address, timestamp, and serialized health and attack predictions. For scalability, large prediction files and historical data are stored on IPFS, with content identifiers (CIDs) recorded on-chain to maintain verifiable links between blockchain events and distributed storage. Performance benchmarking shows that PureChain's Proof-of-Authority (PoA^2) consensus achieves significantly lower latency and higher throughput compared to Ethereum's Proof-of-Stake IV-1, while eliminating transaction costs. This makes PureChain more suitable for real-time, high-frequency IoMT logging.

Explainable AI (XAI) Integration: To enhance trust and transparency, **RemoteCare** integrates SHapley Additive exPlanations (SHAP) into the health and attack prediction pipeline. SHAP values approximate the marginal contribution of each feature x_i to the model's prediction $f(x)$, formulated as:

$$f(x) = \phi_0 + \sum_{i=1}^{M} \phi_i x_i,$$

where ϕ_i represents the Shapley value of feature i, derived from cooperative game theory. These values quantify how each feature contributes to shifting the prediction away from the model's expected baseline ϕ_0.

In practice, SHAP's DeepExplainer was applied separately to the *network branch*, the *health branch*, and the fused representation, allowing attribution of predictions to their most influential features. For example, high packet jitter and abnormal load were consistently identified as strong contributors to attack detection, whereas SpO_2 levels and elevated heart rate were key drivers of critical health predictions. This dual-level interpretability provides both *local explanations* (e.g., why a particular patient instance was flagged Critical or why a traffic flow was classified as malicious) and *global explanations* (e.g., which features consistently influence outcomes across the dataset). Local interpretability supports clinician confidence in individual prediction, while global insights guide system-wide policy tuning and feature engineering. SHAP outputs were visualized using summary plots for global analysis and force plots for patient-level interpretation. By integrating SHAP across both tasks, RemoteCare not only improves the transparency of AI-driven predictions but also delivers actionable insights into the underlying physiological deterioration and cyberattack patterns, ensuring robustness in dynamic IoMT environments.

A. Data Preprocessing and Experimental Setup

Dataset Description: We evaluate the proposed **RemoteCare** framework using the WUSTL-EHMS-2020 dataset [9], which combines synchronized physiological signals with network traffic features. The dataset contains 16,318 samples, covering both benign and malicious traffic, alongside vital signs collected from an IoMT emulation environment. This joint feature space enables simultaneous health and attack classification.

TABLE II
CNN-GRU-LSTM MODEL PARAMETERS

Parameter	Value
Input window size (T)	60
CNN filters (kernel=1)	64
GRU units	64
LSTM units	32
Fusion dense units	64
Dropout (fusion)	0.5
Optimizer	Adam (lr=0.001)
Batch size	256
Epochs	100
Loss	BCE (attack), CE (health)
Early stopping patience	10

Data Preprocessing Non-numeric entries in physiological features were coerced into numeric values, while missing values were imputed with the column mean. Each physiological sample $x^{(h)}$ was mapped to a discrete health class $y^{(h)}$ (Normal, Warning, Critical) using clinically accepted thresholds based on the National Early Warning Score (NEWS) [13]:

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

For network intrusion detection, attack labels were consolidated into a binary mapping: $\{0 : \text{Normal}, 1 : \text{Attack}\}$. To preserve temporal dependencies, a sliding window of $T = 60$ timesteps was applied, yielding inputs $X^{(n)} \in \mathbb{R}^{T \times F_n}$ and $X^{(h)} \in \mathbb{R}^{T \times F_h}$, where $F_n = 10$ and $F_h = 5$ are the top-ranked features by importance. Min–max normalization was applied independently to each channel.

1) Experimental Setup: The dataset was partitioned into training (70%), validation (15%), and test (15%) sets with stratification to maintain class distribution. The hybrid CNN–GRU–LSTM model was implemented in Python 3.10 with TensorFlow/Keras 2.11, Scikit-learn 1.2, and SHAP 0.41. Blockchain logging was deployed on the PureChain network (PoA^2 consensus) using Solidity 0.8.20 and Web3.py 6.0, with Ethereum (PoS) used as a baseline for performance comparison. Model hyperparameters are summarized in Table II. Training was conducted on a workstation equipped with an Intel Core i9-12900K CPU @ 3.20 GHz, 64 GB RAM, and an NVIDIA RTX 3090 GPU (24 GB). Model selection was based on the validation macro-F1 score.

IV. Result Discussion and Performance Evaluation

Table III compares the proposed **RemoteCare** framework against baseline and state-of-the-art models for health and attack classification. For physiological prediction, earlier works such as CNN [14], SVM [15], and LSTM [16] achieved accuracies ranging from 90.0% to 94.2%. In contrast, RemoteCare attained **99.7% accuracy**, 100% precision, 99.4% recall, and 100% F1-score, demonstrating superior capability to discriminate between Normal, Warning, and Critical states. For attack detection, prior studies such as CNN [4], RF [9], [10], and DQN [5] achieved accuracies in the 85–95% range, while the best-performing ensemble model by Gupta et al. [17] reached 99.4% accuracy but lacked health monitoring. RemoteCare delivered **96.0% accuracy**, 96.0% precision, 99.0% recall, and 98.0% F1-score, achieving a favorable precision–recall balance. Compared to CNN-LSTM baselines, RemoteCare reduced false positives while maintaining high recall, ensuring robustness against missed attacks. These results confirm that RemoteCare not only outperforms single-domain baselines but also uniquely provides dual-task prediction in a unified framework.

1) The Blockchain Integration Performance: The PureChain auditability of RemoteCare was benchmarked on both Ethereum Mainnet (PoS) and PureChain (PoA^2), with results summarized in Table IV. Ethereum incurred high latency (6.572 s), limited throughput (15.21 TPS), and non-negligible transaction costs ($0.41–$1.50+ per transaction). In contrast, PureChain achieved **0.2572 s latency**, **69.03 TPS**, and **zero transaction cost**, validating its suitability for high-frequency IoMT logging. These improvements arise from PureChain's consensus algorithm (PoA^2), which is optimized for scalability and low-cost operation in permissioned networks. Thus, while Ethereum demonstrates security maturity, PureChain enables the real-time, cost-free, and scalable audit trail required in mission-critical healthcare applications.

To enhance transparency, RemoteCare integrates SHAP-based XAI to attribute predictions to input features. For health predictions, SHAP identified `Heart_rate`, `Resp_Rate`, and SpO_2 as the dominant drivers of Normal, Warning, and Critical classification, Fig 3. For attack detection, features such as `Packet_num`, `DstJitter`, and `Load` were identified as highly influential in distinguishing malicious traffic from benign flows, see Fig 2. These attributions confirm that the model leverages clinically and technically meaningful features, providing interpretable outputs to clinicians and operators. By embedding explainability at both the health and security layers, RemoteCare addresses the transparency gap left by earlier IDS-focused or health-only systems, thereby strengthening trust and accountability in real-time IoMT monitoring.

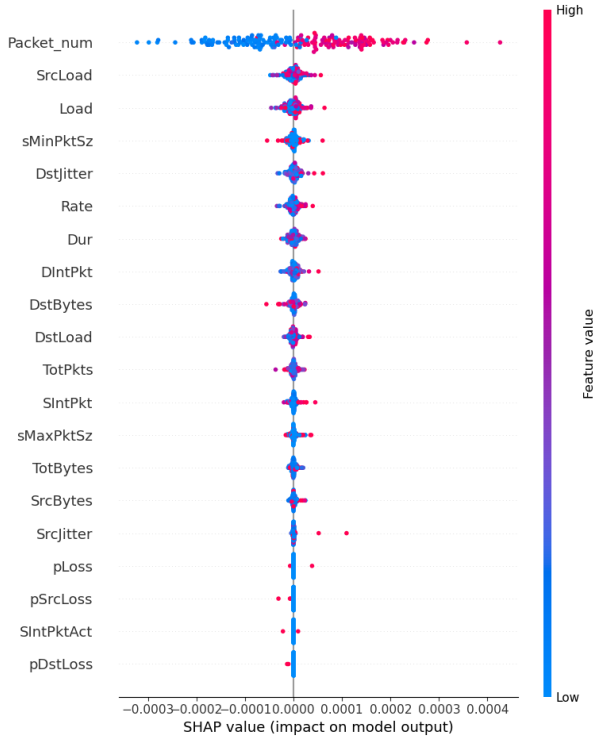

Fig. 2. SHAP summary plot: Top network features impacting attack prediction. Features with higher absolute SHAP values have greater influence on the model output.

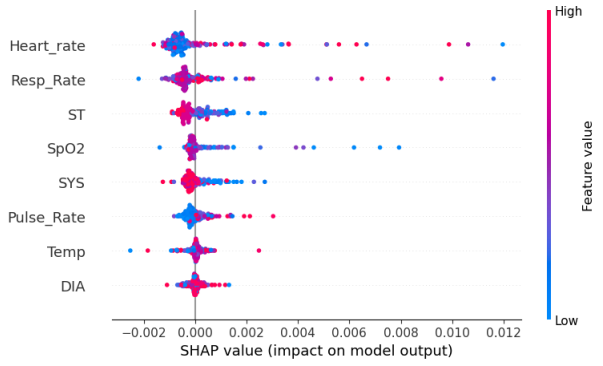

Fig. 3. SHAP summary plot: Physiological features contributing to health status prediction. Key drivers include `Heart_rate`, `Resp_Rate`, and `SpO2`.

V. Conclusion

This paper introduced **RemoteCare**, a blockchain-assisted, explainable deep learning framework designed to address the dual challenges of health state prediction and cyberattack detection in IoMT environments. By integrating a CNN–GRU–LSTM hybrid model with SHAP-based interpretability and PureChain blockchain auditability, RemoteCare ensures accurate, transparent, and tamperproof monitoring. Experimental evaluation showed that RemoteCare achieved 99.7% accuracy in health classification and 96.0% accuracy in attack detection, surpassing prior state-of-the-art models. Blockchain benchmarking confirmed that PureChain significantly reduces latency and transaction costs compared to Ethereum, enabling real-time, cost-free logging. These results demonstrate both the technical robustness and operational feasibility of the proposed

TABLE III
COMPARISON OF PHYSIOLOGICAL (HEALTH) AND ATTACK PREDICTION PERFORMANCE OF MODELS

Reference	Model	Physiological (Health) Prediction				Attack Prediction			
		Acc.	Prec.	Recall	F1	Acc.	Prec.	Recall	F1
[14]	CNN	90.00	90.00	95.00	92.00	–	–	–	–
[15]	SVM	94.20	93.50	95.00	94.20	–	–	–	–
[5]	DQN	–	–	–	–	92.40	–	–	–
[9]	RF	–	–	–	–	94.50	–	–	–
[17]	Ensemble (DT/RF/XGB/ET/GB)	–	–	–	–	99.44	99.76	99.45	0.996
[6]	XGB	–	–	–	–	92.60	92.80	92.60	92.60
RemoteCare (Ours)	CNN–GRU–LSTM	**99.70**	**100.00**	**99.40**	**100.0**	**96.00**	**96.00**	**99.00**	**98.00**

TABLE IV
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)

framework. Future work will focus on extending RemoteCare with federated learning for privacy-preserving training, multi-site deployment for scalability, integration of additional clinical features, and the incorporation of an automated alarm system to enable proactive intervention in critical health states.

ACKNOWLEDGMENT

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government(MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program(IITP-2025-RS-2024-00438430, 34%).

REFERENCES

[1] P. Jayant, E. Vincent, Mohana, M. Moharir, and A. K. A R, "Smart health monitoring and anomaly detection using internet of things (iot) and artificial intelligence (ai)," in *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, 2024, pp. 479–485.

[2] O. Ibrahim Obaid and S. Salman, "Security and privacy in iot-based healthcare systems: A review," *Mesopotamian Journal of Computer Science*, vol. 2022, 04 2023.

[3] S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, M. A. Dini, I. U. Uchechi, D.-S. Kim, and J. M. Lee, "Medical iot record security and blockchain: Systematic review of milieu, milestones, and momentum," *Big Data and Cognitive Computing*, vol. 8, no. 9, p. 121, 2024.

[4] 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. 131 605–131 620, 2024.

[5] L. A. Daher, "Towards secure iomt: Attack detection using deep q-learning in healthcare networks," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, 2023, pp. 407–412.

[6] M. M. Alani, A. Mashatan, and A. Miri, "Explainable ensemble-based detection of cyber attacks on internet of medical things," in *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2023, pp. 0609–0614.

[7] M. A. Dini, S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, I. U. Uchechi, G. A. Haryadi, M. A. P. Putra, D.-S. Kim, T. Jun *et al.*, "Patient-centric blockchain framework for secured medical record fidelity and authorization," *Conference of the Korea Communications Association*, pp. 300–301, 2023.

[8] O. O. Deji-Oloruntoba, J. O. Balogun, T. O. Elufioye, and S. O. Ajakwe, "Hyperuricemia and insulin resistance: Interplay and potential for targeted therapies," *International Journal of Translational Medicine*, vol. 5, no. 3, p. 30, 2025.

[9] 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. 106 576–106 584, 2020.

[10] G. X. Wong, H. Tung Yew, J. A. Diargham, F. Wong, M. Mamat, and S. K. Chung, "Iomt real-time health monitoring system," in *2023 12th International Conference on Awareness Science and Technology (iCAST)*, 2023, pp. 269–273.

[11] C. A. Nnadiekwe, V. I. Kalu, G. C. Akor, and D.-S. Kim, "Blockchain-enabled lightweight data management in smart factories," in *2025 Korea Institute of Communications and Information Sciences*, 2025, pp. 0567–0568. [Online]. Available: https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE12132120

[12] I. Saviour Igboanusi, Allwinnaldo, R. Naufal Alief, M. Rasyid Redha Ansori, J.-M. Lee, and D.-S. Kim, "Ethereum based storage aware mining for permissioned blockchain network," in *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2022, pp. 161–166.

[13] 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," Bournemouth University, Tech. Rep., 2013. [Online]. Available: https://eprints.bournemouth.ac.uk/25324/26/Smith.%20NEWS.pdf

[14] H. Lu, X. Feng, and J. Zhang, "Early detection of cardiorespiratory complications and training monitoring using wearable ecg sensors and cnn," *BMC Medical Informatics and Decision Making*, vol. 24, 2024.

[15] J. Zhang, "Health monitoring and safety early warning system for foundation pit support structure using support vector machine and ensemble learning algorithm," in *2025 IEEE International Conference on Electronics, Energy Systems and Power Engineering (EESPE)*, 2025, pp. 1270–1274.

[16] P. Chen and J. Li, "Construction of a physical health monitoring platform for adolescents driven by big data," in *2024 4th International Conference on Information Technology and Contemporary Sports (TCS)*, 2024, pp. 120–123.

[17] 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 Journal of Biomedical and Health Informatics*, pp. 1–9, 2023.