VIGIL: Blockchain-Assisted Anomaly-Aware Framework for Unified Cyberattack Detection and Cardiopulmonary Monitoring

Chigozie Athanasius Nnadiekwe[1], Simeon Okechukwu Ajakwe(SMIEEE)[1], Jae Min Lee(MIEEE)[1], Dong-Seong Kim(SMIEEE)[1] *

[1] IT-Convergence Engineering, *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 real-time healthcare monitoring but remains vulnerable to anomalies and evolving cyberattacks. We present VIGIL, a blockchain-assisted anomaly-aware framework that unifies intrusion detection and cardiopulmonary risk assessment in a single pass. VIGIL employs dual self-supervised autoencoders with Conv1D/LSTM encoders to enhance resilience against sensor drift, novel threats, and comorbidities while remaining edge-efficient. On WUSTL-EHMS-2020 dataset, VIGIL achieves strong intrusion detection (Acc=88.3%, Rec=0.969, F1=0.928) and near-perfect health classification (Acc=99.95%, κ=0.9982), with 100% recall for critical states. All predictions are immutably logged on PureChain, ensuring tamper-proof auditability and trustworthy IoMT decision support.**

***Index Terms*—IoMT, cardiopulmonary monitoring, intrusion detection, anomaly detection, autoencoder, PureChain.**

I. INTRODUCTION

The IoMT enables real-time acquisition of cardiopulmonary signals such as heart rate, SpO_2, respiratory rate, and blood pressure, using interconnected sensors and devices, supporting early detection of deterioration in both clinical and military contexts [1], [2]. However, current IoMT frameworks are constrained by reliance on supervised deep learning with clean, labeled datasets, limiting robustness under noisy signals, sensor drift, and comorbidities [3]. Moreover, IoMT connectivity exposes critical vulnerabilities to spoofing, tampering, and denial-of-service attacks, while many systems lack integrated intrusion detection and immutable audit mechanisms [4]. These limitations underscore the need for frameworks that combine clinical monitoring with anomaly and security awareness. Hence, the motivation of this study.

Recent works suggests promising directions. Unsupervised autoencoder-based approaches can detect unseen anomalies without extensive labeled data, capturing deviations from baseline physiological or network behavior [5]. Also,blockchain has emerged as a tamper-resistant backbone for IoMT, offering auditability, decentralized trust, and role-restricted access control [6]. Furthemore, blockchain-assisted intrusion detection frameworks demonstrate improved resilience against malicious traffic in heterogeneous IoMT environments [7], while clinical reviews emphasize that remote monitoring systems must balance accuracy in health triage with strong guarantees of data integrity and trustworthiness [3], [8]. To this end, we present *VIGIL*, a blockchain-assisted anomaly-aware framework that integrates self-supervised autoencoders with Conv1D and long short term memory (LSTM) encoders for simultaneous cardiopulmonary monitoring and cyberattack detection, with all outputs immutably logged on PureChain [6] for forensic traceability.

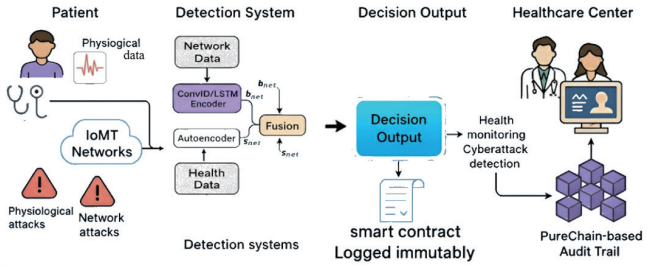

Fig. 1. Overview of VIGIL system highlighting IoMT integration, dual-path anomaly detection, and blockchain audit logging.

II. PROPOSED METHODOLOGY

For synchronized input windows, network features x_{net} and vitals x_{hlt} are standardized:

$$x_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j + \epsilon}, \quad \epsilon > 0. \tag{1}$$

Supervised encoders (Conv1D for x_{net}, LSTM for x_{hlt}) are fused with anomaly-sensitive bottlenecks from autoencoders. The joint embedding h drives two heads:

$$\hat{y}_{\text{att}} = \sigma(W_{\text{att}} h + b_{\text{att}}), \tag{2}$$

$$\hat{y}_{\text{hlt}} = \text{softmax}(W_{\text{hlt}} h + b_{\text{hlt}}). \tag{3}$$

The hybrid objective combines anomaly reconstruction and supervised losses:

$$\mathcal{L} = \lambda_{\text{AE}}(\mathcal{L}^{\text{AE}}_{\text{net}} + \mathcal{L}^{\text{AE}}_{\text{hlt}}) + \lambda_{\text{att}}\mathcal{L}_{\text{BCE}}(y_{\text{att}}, \hat{y}_{\text{att}}) + \lambda_{\text{hlt}}\mathcal{L}_{\text{CE}}(y_{\text{hlt}}, \hat{y}_{\text{hlt}}). \tag{4}$$

A. Blockchain Audit Layer

To ensure traceability, each inference $(\hat{y}_{\text{att}}, \hat{y}_{\text{hlt}})$ is serialized and immutably logged on the PureChain blockchain. A role-restricted smart contract enforces controlled write access (`LOGGER_ROLE`), while logs store compact byte payloads encoding probabilities and health classes. This design guarantees tamper-evident auditability and supports forensic verification during anomalous or malicious events (Fig. 1).

III. Results and Discussion

On WUSTL-EHMS-2020 with 70/15/15 splits, as shown in Table I, *VIGIL* achieved strong attack detection (Acc = 0.8827, Prec = 0.8911, Rec = 0.9686, F1 = 0.9282, ROC = 0.8449). Calibration curves (Fig. 2) confirm well-calibrated attack probabilities.

TABLE I
ATTACK DETECTION COMPARISON (BEST PER ROW IN **BOLD**).

Model	Acc	Prec	Rec	F1	ROC
VIGIL	**0.8827**	0.8911	**0.9686**	**0.9282**	0.8449
AE–CNN–GRU	0.8784	**0.8920**	0.9611	0.9253	0.8388
BiLSTM	0.8867	**0.8926**	0.9724	0.9308	**0.8453**
CNN	0.8807	0.8828	**0.9774**	0.9277	0.8423
Transformer	0.8454	0.8633	0.9535	0.9062	0.8141

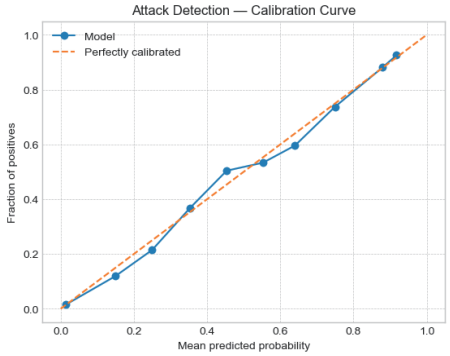

Fig. 2. Calibration curve of the attack detection task for **VIGIL**.

For health status classification, VIGIL attained Acc = 0.9995, ROC-AUC (macro) = 0.999963, and $\kappa = 0.9982$, with performance comparable to AE–CNN–GRU.

TABLE II
HEALTH STATUS CLASSIFICATION (BEST PER ROW IN **BOLD**).

Metric	VIGIL	AE–CNN–GRU
Accuracy	0.9995	**0.9996**
ROC-AUC (macro)	**0.999963**	0.999956
ROC-AUC (micro)	**0.999996**	**0.999996**
Cohen's	0.9982	**0.9984**

Table II and Fig. 3 shows that both VIGIL and AE–CNN–GRU deliver near-perfect health classification, with accuracies exceeding 99.9%. Although AE–CNN–GRU reports marginally higher accuracy and κ, these differences are clinically insignificant, while VIGIL's superior macro ROC–AUC demonstrates more consistent discrimination across all health states, justifying its adoption for robust IoMT monitoring.

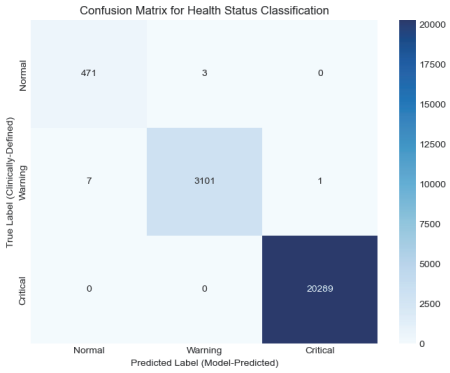

Fig. 3. Confusion matrix of VIGIL health classification (3 classes).

Table III shows that the PureChain network achieved a mean latency of 229.3 ms and throughput of 14.1 TPS, confirming its capability for real-time, low-latency dual-task logging. These metrics demonstrate that the blockchain layer efficiently supports high-frequency IoMT prediction updates without performance bottlenecks.

TABLE III
BLOCKCHAIN LOGGING METRICS ON PURECHAIN FOR DUAL-TASK

Metric	Mean	Range
Latency (ms)	229.3	140–376
Throughput (TPS)	14.1	6–18

IV. Conclusion

We presented *VIGIL*, a blockchain-assisted anomaly-aware IoMT framework that unifies cardiopulmonary monitoring and intrusion detection. By fusing Conv1D, LSTM, and self-supervised autoencoders, VIGIL balances security sensitivity (high recall for attacks) and clinical safety (100% recall for critical states). All outputs were immutably logged to PureChain, ensuring auditability. By uniting clinical safety with security sensitivity, VIGIL strengthens IoMT resilience and paves the way for broader validation and clinical integration.

Acknowledgment

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

References

[1] C. A. Nnadiekwe, C. I. Okafor, J.-M. Lee, and D.-S. Kim, "Soldiercare: Blockchain-enabled iomt framework for real-time health monitoring and cyberattack detection in tactical environments," in *The 4th International Conference on Mobile • Military • Maritime IT Convergence*, 2025.

[2] T. P. Theodore Armand, M. A. I. Mozumder, K. S. Carole, O. Deji-Oloruntoba, H.-C. Kim, and S. O. Ajakwe, "Elipf: Explicit learning framework for pre-emptive forecasting, early detection and curtailment of idiopathic pulmonary fibrosis disease," *BioMedInformatics*, vol. 4, no. 3, pp. 1807–1821, 2024.

[3] C. A. Nnadiekwe, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Remotecare: Secure and explainable dual-task health and cyberattack detection framework for iomt," in *Proceedings of the 16th International Conference on ICT Convergence (ICTC)*. Jeju, South Korea: IEEE, October 2025.

[4] 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.

[5] H. Park, D. Shin, C. Park, J. Jang, and D. Shin, "Unsupervised machine learning methods for anomaly detection in network packets," *Electronics*, vol. 14, no. 14, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/14/2779

[6] I. S. Igboanusi, C. A. Nnadiekwe, J. U. Ogbede, D.-S. Kim, and A. Lensky, "Boms: blockchain-enabled organ matching system," *Nature Scientific Reports*, vol. 14, 07 2024. [Online]. Available: https://doi.org/10.1038/s41598-024-66375-5

[7] B. Zaabar, O. Cheikhrouhou, and M. Abid, "Intrusion detection system for iomt through blockchain-based federated learning," in *2022 15th International Conference on Security of Information and Networks (SIN)*, 2022, pp. 01–08.

[8] 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.