JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), MARCH, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

Anomaly Detection on Clinical IOT and Embedded Devices using Deep Learning

[1]Ahmadu Mohammed Girei, [2]Nurudeen M. Ibrahim, [3]Prema Kirubakaran, [4]Muhammad Aliyu Suleiman, [5]Adamu Garba Abdullahi, [6]Shittu Abdulrahman, [7]Faruku Umar Ambursa
[1&3]Department of Information Technology, Nile University of Nigeria
[2&5]Department of Cybersecurity Nile University of Nigeria
[4]Department of Computer Nile University of Nigeria
[6]Department of Computer Science, Ahmadu Bello University Zaria, Kaduna
[7]Department of Information Technology, Bayero University Kano

ABSTRACT
The sudden increase in the adoption of the Internet of Medical Things (IoMT) has greatly improved the quality of healthcare delivery; however, it has also introduced new cybersecurity threats capable of jeopardizing patient safety. Conventional intrusion detection systems and traditional machine learning (ML) techniques face significant limitations in IoMT environments due to their high computational requirements and challenges associated with class imbalance. This study developed an optimized deep learning-based intrusion detection model to improve anomaly detection in resource-constrained IoMT networks using the CICIoMT2024 dataset. The study explored the implementation of an efficient separable One-Dimensional Convolutional Neural Network (1D-CNN) combined with focal loss to address the issue of class imbalance across the 19-class attack taxonomy. The results showed that the proposed separable 1D-CNN achieved a high classification accuracy of 98.54% while maintaining minimal computational resource usage. In addition, the detection of minority attacks, such as spoofing and reconnaissance port scanning, achieved a recall of 64% and an F1-score of 91% through the use of focal loss. The study concluded that lightweight deep learning architectures enhanced with separable convolutions and focal loss can provide an effective and scalable solution for securing IoMT devices and safeguarding patients from cyber threats.

ARTICLE INFO
Article History
Received: November, 2025
Received in revised form: December, 2025
Accepted: February, 2026
Published online: March, 2026

KEYWORDS
IoMT, Cybersecurity, Anomaly Detection, Deep Learning, 1D-CNN, Separable Convolutions

INTRODUCTION

In recent times, the healthcare sector has witnessed significant transformation due to the increasing adoption of the Internet of Medical Things (IoMT) Internet of Medical Things (Saxena & Mittal, 2022). Diagnosis and patient care have greatly improved because medical devices are now interconnected in ways that enhance healthcare delivery and monitoring. Despite these benefits, the rise of IoMT has also introduced serious cybersecurity risks from malicious actors. Improper implementation of communication protocols used in connecting medical devices can create vulnerabilities with severe consequences (Karam, 2022). In traditional networks, Intrusion Detection Systems (IDSs) and machine learning algorithms are commonly used to detect and prevent zero-day attacks; however, in IoMT environments, these methods often fall short due to the large volume of traffic generated by modern IoMT devices (Bouriche & Bouriche, 2022).

The foregoing highlights the need for more effective approaches to mitigating cyberattacks in IoMT environments. Since conventional machine learning algorithms have limitations in handling complex and high-volume

Corresponding author: Ahmadu Mohammed Girei
ahmuhammad500@gmail.com
Department of Information Technology, Nile University of Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), MARCH, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

IoMT traffic, deep learning models such as Convolutional Neural Networks (CNNs) Convolutional Neural Network provide a promising alternative. This is mainly due to their ability to automatically extract temporal and spatial features from raw network traffic, thereby improving attack detection capabilities.

The motivation for the development of this optimized anomaly detection system is based on the following factors:

i. Computational Resource Constraints: Modern medical IoT devices often have limited processing power, memory capacity, and battery life, making the deployment of standard CNN models difficult because of their high computational requirements.
ii. High Class Imbalance and Minority Attack Detection Failure: IoMT network traffic is highly imbalanced, with dominant attack classes such as Distributed Denial of Service (DDoS) significantly outweighing other attack categories, while less frequent but dangerous minority attack classes such as reconnaissance and spoofing often remain undetected.

In view of the above, the proposed system seeks to contribute to ongoing efforts aimed at securing IoMT networks. The aim of this study is to develop a deep learning model for anomaly detection in medical IoT environments. The objectives of the study is to design a deep learning model using an optimized CNN architecture. The remainder of the paper is organised as follows: section 2 presents the literature review, section 3 discusses about the methodology, section 4 presents the result while section 5 concludes the paper.

Related Work

Deep learning models have, over time, proven to be reliable and advanced alternatives to traditional Intrusion Detection Systems (IDSs) that rely on pre-existing signatures, as they can continuously evolve to adapt to emerging threat vectors (Juyal et al., 2023).Specifically, One-Dimensional Convolutional Neural Networks (1D-CNNs) One-Dimensional Convolutional Neural Network excel at automatically extracting complex features from the sequential and time-series nature of network data packets. Dadkhah et al. (2024) benchmarked the CICIoMT2024 dataset using traditional machine learning algorithms and revealed significantly low performance, with classification accuracy below 73% across 19 attack classes, indicating poor effectiveness in identifying complex attack types. Mohammadi et al. (2024) explored the use of standard CNNs for medical IoT threat detection and achieved high accuracy of approximately 99%; however, these architectures rely on standard convolution operations that require substantial computational resources, making them unsuitable for resource-constrained edge devices and thereby creating a research gap in lightweight and class imbalance-aware solutions.

METHODOLOGY

The methodology explains the approach adopted by the researcher to achieve the aim and objectives of the project. It highlights the methods used for data collection, model selection, data preprocessing, and system development. The CICIoMT2024 benchmark dataset was used in developing the proposed model (Dadkhah et al., 2024). The dataset contains a combination of 18 different cyberattacks and benign traffic generated from 40 distinct IoMT devices. To address resource constraints, Depthwise Separable Convolutions Depthwise Separable Convolution were utilized in the development of the model (Mazhar et al., 2023). This approach separates standard convolution operations into depthwise and pointwise convolutions, thereby significantly reducing the number of parameters and computational costs.

Preprocessing involved the following stages:

i. Label Encoding: All attack categories were assigned numerical integer labels and then One-Hot Encoded for multi-class classification.
ii. Standardisation: Feature values were normalized using StandardScaler to achieve a mean of 0 and a standard deviation of 1.

Corresponding author: Ahmadu Mohammed Girei
ahmuhammad500@gmail.com
Department of Information Technology, Nile University of Nigeria.

iii. Reshaping: The standardized 2D data was reshaped into a 3D tensor to meet the input requirements of the 1D Convolutional layers.

Model training and evaluation involved the following procedures:

i. Data Splitting: The CICIoMT2024 benchmark dataset was divided into a training set (80%) and a testing set (20%).
ii. Model Fitting: The 1D-CNN model One-Dimensional Convolutional Neural Network was trained using Focal Loss to address the issue of extreme class imbalance. The imbalance was handled by down-weighting well-classified examples and directing the model's learning process toward difficult and misclassified instances.
iii. Evaluation: The model was evaluated using quantitative performance metrics derived from the confusion matrix.

The design of the proposed system consisted of the following:

i. Programming Languages/Frameworks: Python 3, TensorFlow, and Keras were used for deep learning model development.
ii. Development Environment: The model was developed on a Kaggle Notebook Runtime utilizing two NVIDIA Tesla T4 GPUs with 16GB memory each.
iii. Key Libraries: Pandas and NumPy were used for data manipulation, while Scikit-learn was used for data preprocessing and evaluation.

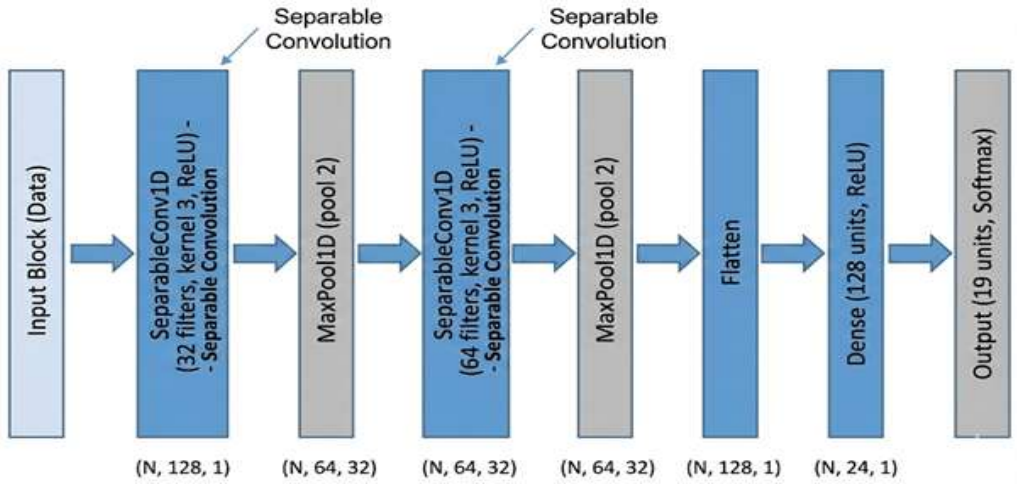

Figure 1: schematic of the Optimized CNN Architecture.

Evaluation Metrics

To determine its effectiveness in classification tasks, the simple 1D-CNN model developed for this project must first be evaluated. The following metrics were used to assess the performance of the 1D-CNN classification system:

i. Accuracy: Accuracy measures the overall percentage of instances that were correctly classified by the model.
ii. Precision: Precision measures the proportion of correctly predicted positive instances, indicating how many of the predicted positive results are actually correct.
iii. Recall (Sensitivity): Recall is the proportion of actual positive instances that were correctly identified by the model, demonstrating how effectively the model detects all positive cases.
iv. F1-Score: The F1-Score is a combined measure of Precision and Recall, providing a balanced evaluation of model performance, particularly when dealing with imbalanced classes.

Corresponding author: Ahmadu Mohammed Girei
ahmuhammad500@gmail.com
Department of Information Technology, Nile University of Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(1), MARCH, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

RESULTS

A very high classification accuracy of 98.54% was achieved after evaluating the results of the 1D-CNN model One-Dimensional Convolutional Neural Network. This indicates that the model performed exceptionally well while significantly reducing computational complexity compared to standard CNN architectures. When tested on high-volume volumetric attacks such as DDoS-ICMP, DDoS-UDP, and DoS-SYN, the model demonstrated near-perfect F1-scores ranging from 0.99 to 1.00. Spoofing attacks and Recon_Port_Scan attacks, which often go undetected using conventional methods, were more effectively identified through the adoption of Focal Loss. The 1D-CNN model developed for this project achieved a recall rate of 64% for Spoofing attacks and an F1-score of 91% for Recon_Port_Scan attacks. Overall, the results demonstrate that this lightweight architecture successfully balances computational efficiency with robust multi-class attack detection.

Table 1: Classification Result

Metric	Value
Accuracy	98.54%
Precision (Weighted)	98.71%
Recall (Weighted)	98.54%
F1-Score (Weighted)	98.34%

The implementation of Focal Loss Focal Loss proved to be more effective in detecting minority attack classes when compared to baseline benchmark models. This improvement is evident from the detailed analysis of the Classification Report across all attack classes.

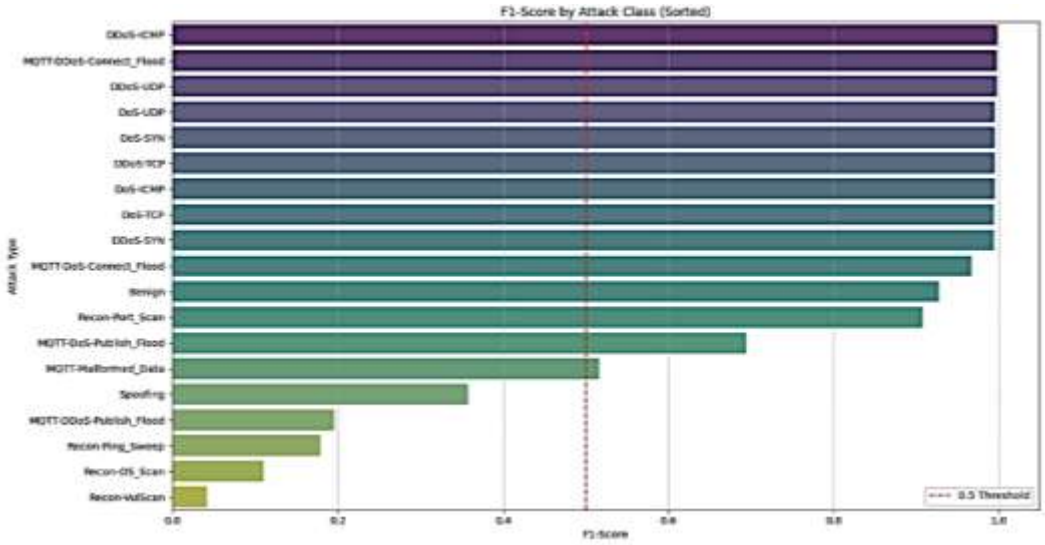

Figure 2 : Class-Wise Analysis

CONCLUSION

This project successfully developed a lightweight 1D-CNN model One-Dimensional Convolutional Neural Network for detecting cyberattacks in IoMT ecosystems. Depthwise separable convolutions Depthwise Separable Convolution were utilized instead of standard convolution operations, yet the model achieved a high accuracy rate of 98.54% while significantly reducing computational complexity. Class imbalance remains a major challenge when using conventional loss functions, often resulting in poor recall for minority attacks such as spoofing. This challenge was effectively addressed through the implementation of Focal Loss Focal Loss instead of traditional loss functions. Future studies should explore hardware-in-the-loop testing, which

Corresponding author: Ahmadu Mohammed Girei
ahmuhammad500@gmail.com
Department of Information Technology, Nile University of Nigeria.

involves deploying the model on physical embedded devices to evaluate inference latency and power consumption. In addition, future research should consider the integration of Explainable Artificial Intelligence (XAI) Explainable Artificial Intelligence techniques to reduce false positives by generating visualizations that highlight the specific packet features responsible for attack detection.

REFERENCES

Bouriche, A., & Bouriche, S. (2022). A Systematic Review on Security Vulnerabilities to Prevent Types of Attacks in IoMT. International Journal of Computations, Information and Manufacturing (IJCIM).

Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. Internet of Things, 28, 101351.

Juyal, A., Bhushan, B., Hameed, A. A., & Jamil, A. (2023). Deep Learning Approaches for Cyber Threat Detection and Mitigation. Proceedings of the 2023 7th International Conference on Advances in Artificial Intelligence.

Karam, A. A. (2022). Investigating the Importance of Ethics and Security on Internet of Medical Things (IoMT). International Journal of Computations, Information and Manufacturing (IJCIM).

Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sciences, 13(4), 683.

Mohammadi, A., Aminian, M., Ghahramani, H., & Asghari, S. A. (2024). Securing Healthcare with Deep Learning: A CNN-Based Model for medical IoT Threat Detection. 2024 19th Iranian Conference on Intelligent Systems (ICIS).

Saxena, A., & Mittal, S. (2022). Internet of Medical Things (IoMT) Security and Privacy: A Survey of Recent Advances and Enabling Technologies. Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing.

Corresponding author: Ahmadu Mohammed Girei
ahmuhammad500@gmail.com
Department of Information Technology, Nile University of Nigeria.