Optimized Feedforward Neural Network for Error Reduction in Medical Internet of Things

Kalibbala Jonathan Mukisa, Love Allen Chijioke Ahakonye [†], Dong-Seong Kim, Jae Min Lee
IT Convergence Engineering, [†] ICT Convergence Research Center,
Kumoh National Institute of Technology Gumi, South Korea
kjonmukisa, loveahakonye, dskim, ljmpaul@kumoh.ac.kr

***Abstract*—This paper addresses the rising vulnerability of the medical Internet of Things (MIoT) to attacks like spoofing and data alteration. Using the focal loss function to enhance neural network models boosts detection accuracy and reduces false positives. Experimental findings on recent MIoT data demonstrate that the focal loss function notably reduces error loss in evaluated feedforward and artificial neural network models.**

***Index Terms*—Artificial neural network, Feedforward neural network, Focal loss, Medical Internet of Things, Machine learning**

I. Introduction

The Internet of Medical Things (IoMT) consists of smart medical devices connected to the Internet of Things (IoT), significantly improving remote patient monitoring and healthcare operations. While IoMT technology has transformed healthcare by providing real-time data collection from diverse heterogeneous sensor sources [1], security remains a critical concern that requires robust security measures [2]. Artificial intelligence-based intrusion detection techniques have proven effective in addressing vulnerabilities, but they require optimization for minimal error and precise detection.

Neural networks, particularly deep learning models, excel at processing complex data and extracting valuable insights, making them ideal for analyzing medical IoT (MIoT) data [3], [4]. However, deploying neural networks in MIoT settings faces challenges due to resource constraints like limited processing power and memory in IoT devices [1]. It necessitates optimized neural network architectures and algorithms to ensure high accuracy and reliability in medical data analysis, which is crucial for minimizing errors in diagnosis, monitoring, and treatment [5].

This study optimizes Feedforward Neural Networks (FNN) and Artificial Neural Networks (ANN) for MIoT applications to minimize error loss and enhance performance metrics like accuracy, recall, f1-score and robustness in medical data analysis tasks such as anomaly detection [5]. By tailoring neural network architectures, training procedures, and inference mechanisms for MIoT environments, we aim to mitigate errors, improve reliability, and foster the development of intelligent MIoT systems. The research outcomes have significant potential to revolutionize healthcare delivery by enabling timely, accurate, and precise analysis. Its relevance is imperative for disease diagnosis, anomaly detection, patient monitoring, and predictive analytics.

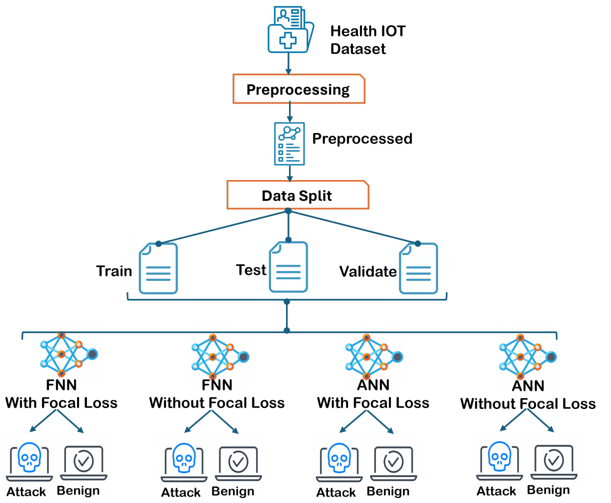


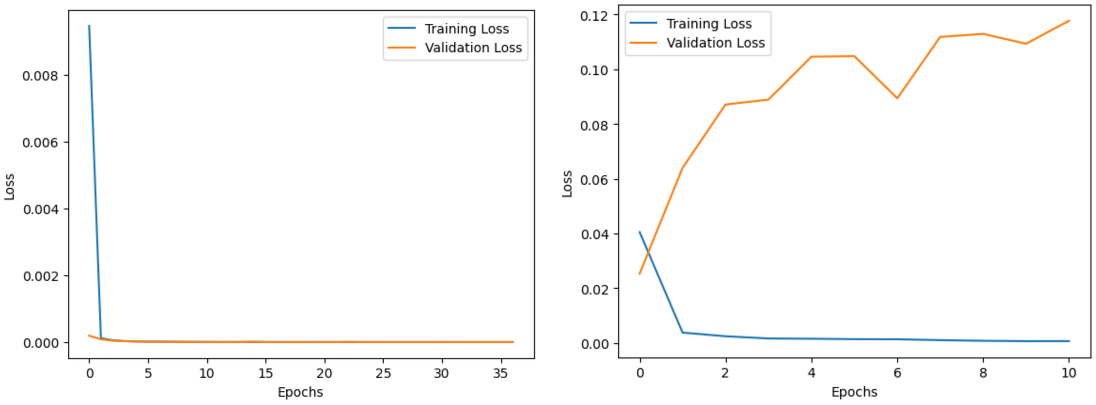
Fig. 1: The Pipeline process flow of the model optimization.

II. System Methodology

This section outlines the system overview in Fig 1, detailing the pipeline process flow. The system comprises two machine learning models trained with the same parameters, facilitating comparative analysis. In the context of MIoT systems, particularly in healthcare, addressing imbalanced datasets is paramount due to the potential consequences of misclassifications. Data imbalance leads to biased predictions and decreased performance in detecting sparse anomalous instances. To mitigate this issue, leveraging the focal loss function prioritizes challenging instances, improving the model's generalization across different classes and enhancing overall performance [5].

This study employed the enhanced healthcare monitoring system (EHMS) dataset, WUSTL EHMS 2020 [6] [1]. It consists of spoofing and data alteration attacks, compromising the confidentiality and privacy of healthcare systems. The data preprocessing eliminated irrelevant features, addressing outliers to enhance the data quality. The model training constitutes FNN and ANN with and without focal loss, the test set evaluates the model performance on unseen data, and the validation set fine-tunes model parameters, preventing overfitting.

[1] https://www.cse.wustl.edu/ jain/ehms/index.html



(a) FNN with focal loss

(b) FNN without focal loss

Fig. 2: Graph demonstrating the learning process path of the FNN with and without focal loss function.

TABLE I: Comparison of model performance on the implementation of Focal Loss for error reduction

	Model Training with Focal Loss		Model Training without Focal Loss	
Metrics	**FNN**	**ANN**	**FNN**	**ANN**
Accuracy (%)	99.98	99.50	99.92	99.92
Precision (%)	99.96	97.44	99.88	99.88
Recall (%)	99.89	95.74	99.05	99.06
F-score (%)	99.92	96.58	99.46	99.47
Loss (#)	**0.0000**	**0.0008**	0.0253	0.0037

The choice of neural networks in this study is consequential upon its flexibility, approximation capabilities, and the ability to handle complex relationships, making them valuable for classification in highly imbalanced and heterogeneous MIoT data. The FNN and ANN network architecture includes two dense layers with 64 and 32, each followed by a ReLU activation function for non-linearity and enhancing the model's capacity to capture complex patterns. The output layer employs the sigmoid activation function to produce probabilistic outputs suitable for binary classification. The model training was optimized by implementing focal loss with 0.2.2 alpha, 2.0 gamma combined with binary_crossentropy to minimize error loss, false positives and computation resources.

III. Performance Evaluation

The evaluated FNN and ANN models with focal loss demonstrated significant performance in minimizing error loss as in Table I with FNN recording 0 loss. Similarly, ANN with focal loss had a 0.0008 error loss. In addition to error reduction, the models achieved high classification accuracy, precision, recall and f-score, as highlighted in Table I. Figure 2 is the learning process path of FNN, showing its performance with and without focal loss. Optimizing machine learning algorithms notably enhances their performance.

IV. Conclusion

This study optimized FNN and ANN models to classify highly imbalanced and heterogeneous MIoT data efficiently. The experimental analysis integrated focal loss to reduce error loss and false positives. Considering the complexity and sparsity of some attack instances of the MIoT data, the optimized FNN with focal loss significantly eliminated error loss with excellent model performance. A future direction is to employ blockchain optimization for secure and immutable medical health information.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-2020-0-01612, 33.3%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33.3%) and This work was supported by (NRF-2022R1I1A3071844, 33.3%).

References

[1] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," *IETE Technical Review*, vol. 39, no. 4, pp. 775–788, 2022.

[2] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Agnostic CH-DT Technique for SCADA Network High-Dimensional Data-Aware Intrusion Detection System," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10 344–10 356, 2023.

[3] J. Mohana, B. Yakkala, S. Vimalnath, P. B. Mansingh, N. Yuvaraj, K. Srihari, G. Sasikala, V. Mahalakshmi, R. Y. Abdullah, and V. P. Sundramurthy, "Application of Internet of Things on the Healthcare Field using Convolutional Neural Network Processing," *Journal of Healthcare Engineering*, vol. 2022, 2022.

[4] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Classification and Characterization of Encoded Traffic in SCADA Network using Hybrid deep Learning Scheme," *Journal of Communications and Networks*, vol. 26, no. 1, pp. 65–79, 2024.

[5] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "X-HDNN: Explainable Hybrid DNN for Industrial Internet of Things Backdoor Attack Detection," in *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, 2023, pp. 1053–1057.

[6] 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.