A SECURE AGGREGATION FRAMEWORK FOR FEDERATED HEALTH CARE DATA MONITORING

[1]Dr. N.Subhashini, [2]A. Hariharan, [3]S. Hariharan, [4]G. Harikaran, [5]C. Jana.

[1]Associate Professor, Department of Electronics and Communication Engineering

[2,3,4,5]Student, Department of Electronics and Communication Engineering,
[1, 2, 3, 4, 5]SRM Valliammai Engineering College, Kattankulathur, Tamil Nadu, India

Abstract : The quick rise of Internet of Things (IoT) technology in healthcare has made it possible to keep track of health data continuously through wearable and built-in devices. To solve the issues with current centralized cloud systems, this study suggests a healthcare monitoring system that keeps user privacy safe by using Federated Learning along with IoT-based health sensors. This system works with ESP32 microcontrollers connected to MAX30102 and TMP117 sensors to gather real-time health data like heart rate, oxygen levels in blood, and temperature of the body. A simple logistic regression model that uses SoftMax is run on each client device to sort health conditions into three groups: Normal, Mild Risk, and Critical. Instead of sending the raw sensor data, the system only shares the model information that has been trained locally with a central server using the Federated Averaging method. Tests show that the system is very accurate. It also shows that it can quickly adapt during training rounds and has low computing requirements, making it suitable for small IoT devices. Overall, the system provides real-time health monitoring with better security, the ability to grow as needed, and protection of personal data.

Index Terms - Federated learning, Healthcare monitoring, Internet of Things, ESP32, Data privacy, Physiological sensors.

1.INTRODUCTION

Modern healthcare systems are using constant monitoring of health signs more and more to keep patients safe and catch health problems early. The physiological data such as heart rate, oxygen level in blood , and body temperature are important signs of how a patient is doing. Older monitoring systems often gather data in one place, sending patient information all the time to a remote server for processing and checking. While this method has great computing power, it creates big problems with keeping data private, secure, and dealing with delays in network communication. Medical information is very private and has to follow strict laws for protection. When raw patient information is sent over networks, it raises the chances of data leaks, unauthorized access, and misuse. Additionally, many traditional healthcare monitoring systems are based on set rules that rely on certain levels to signal warnings. These systems don't change based on each patient's unique needs, which can lead to false alarms or missing important warning signs.

To solve this issue, this study presents a federated learning (FL) system that works with IoT-based health monitoring devices. Federated learning is a method of training machine learning models that focuses on keeping data private. In this system, models are trained directly on devices close to the patients, and only the improved model information is sent to a central server. This method improves privacy, lowers the quantity of data to be sent, and makes it easier to apply in different hospital areas.

2.LITERATURE STUDY

Recent advancements highlight the critical role of decentralized intelligence in healthcare. Research conducted by Arikumar et al. [1] and Elayan et al. [3] demonstrates that using federated learning with wearable health devices can significantly reduce privacy risks while maintaining effective communication within Internet of Things networks. Moreover, a study by Baghersalimi et al. [2] on detecting epileptic seizures confirms that decentralized model training using random optimization ensures the safety of individual patient information without compromising the accuracy of diagnosis. When examining continuous body signals, Brophy and their team [4] effectively applied federated learning to estimate blood pressure using PPG sensors, adhering to data protection regulations. Additionally, Chen [5] developed cybersecurity frameworks specifically for home monitoring systems for the elderly, integrating IoT and federated learning.

The foundational ideas behind these developments were introduced by McMahan et al. [6], who emphasized communication-efficient learning of deep networks from decentralized data.

This was further structured by Konečný et al. [7], who concentrated on federated optimization for on-device intelligence. The general concepts, applications, and challenges of federated machine learning have been thoroughly reviewed by Yang et al. [8] and Li et al. [9], underscoring its significant potential in distributed computing systems. Furthermore, Kairouz et al. [10] outlined the ongoing progress and open challenges in the field, supporting its secure implementation in critical sectors.

In the context of digital health, Rieke et al. [11] discussed the transformative potential of federated learning in medical applications.Since security remains a top priority in medical data, Xu et al. [12] and Liu et al. [13] created secure and efficient frameworks using differential privacy tailored for IoT-based healthcare systems. The reliability of federated learning over wireless networks has also been shown by Chen et al. [14], who introduced joint learning and communication frameworks, and Pokhrel and

Choi [15], who examined federated learning combined with blockchain to illustrate the broader need for secure, decentralized communication structures. Building on these established security methods and communication frameworks, our proposed system employs a SoftMax-based logistic regression model trained across ESP32 sensing devices to guarantee secure and timely health classification.

3. SYSTEM DESIGN AND METHODOLOGY

3.1System Architecture

The suggested system for monitoring health while keeping privacy safe is made using a spread-out learning setup. This system has several client units, each working with an ESP32 microcontroller connected to health sensors, plus a main server that brings everything together. This design guarantees that the original patient information stays on the local device and is not sent elsewhere, the Figure 1 shows the overall system architecture for physiological monitoring.

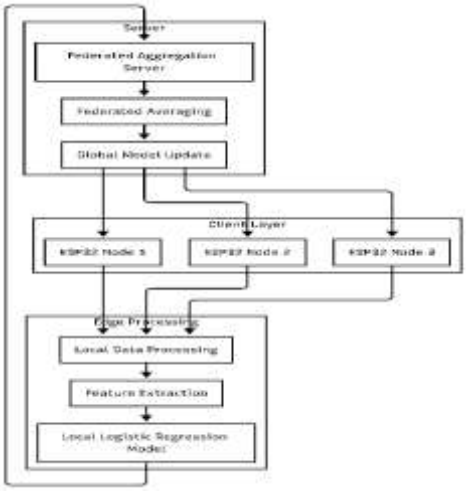

Figure 1: Overall federated learning system architecture for physiological monitoring

3.2 Hardware Components and Data Acquisition

The ESP32 microcontroller is the main part of each client node, giving it the power to run simple machine learning programs. It connects with a MAX30102 sensor using I2C to collect PPG signals that help estimate heart rate and oxygen levels in the blood. A TMP117 temperature sensor is used to check body temperature, which is accurate to about ±0.1°C. The raw signals go through digital filtering to reduce disturbances from movement and background noise before they are turned into organized feature vectors.

3.3 Machine Learning Model Implementation

A multiclass logistic regression model based on SoftMax was chosen because it is easy to compute and works well on small devices. Let's say we have an input feature vector that looks like this: x = [heart rate, SpO2, temperature]. The model determines how likely each health status is by using the SoftMax function:

$$P(x) = \frac{expexp\,(w_k \cdot x + b_k)}{\sum \quad expexp\,(w_j \cdot x + b_j)}$$

In this function, w_k is the weight for class k, and b_k is the bias. While training the model, we use a method called stochastic gradient descent to change the model weights step by step, aiming to reduce the cross-entropy loss. The system places patients into three groups based on their conditions: Normal, Mild Risk, and Critical.

3.4 Federated Learning Algorithm

The federated learning process happens in several rounds of communication as shown in Figure 2. For a set number of training cycles each client node start training the model with the data available with it. Once the training is done, only the new model updates are sent way back to the server. The server then aggrgates these updates using a method called Federated Averaging, or FedAvg. If there are a total of N client nodes, the new global model weights are figured out like this:

$$W_{global} = \frac{1}{N} \sum_{i=1}^{N} \quad W_i$$

Here, W_i stands for the weights coming from client i. After the model is combined, it is sent out again to all clients for the following round.

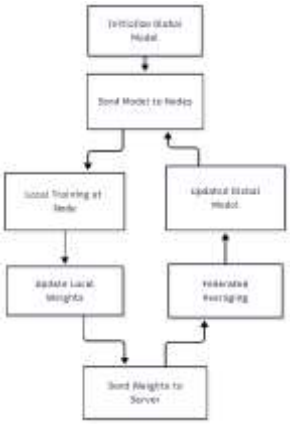

Figure 2: Federated learning training and aggregation workflow

4. RESULTS AND DISCUSSION

4.1 Sensor Performance and Local Training

The MAX30102 sensor showed that the heart rate could change by about ±2 beats per minute and that the oxygen level had a difference of ±1–2% when things were steady, which proves that the hardware is dependable. At first, it was tested in a controlled training environment, and the cross-entropy loss went down steadily over time, which means it was consistently improving.

4.2 Federated Learning Training Results

After collecting data using Federated Averaging, the overall model showed steady improvement in its ability to classify during each round of communication. Figure 3 shows that the federated model reached a total accuracy of 99.17%, which is similar to what you get with centralized training, all while keeping the original physiological data safe on individual devices.

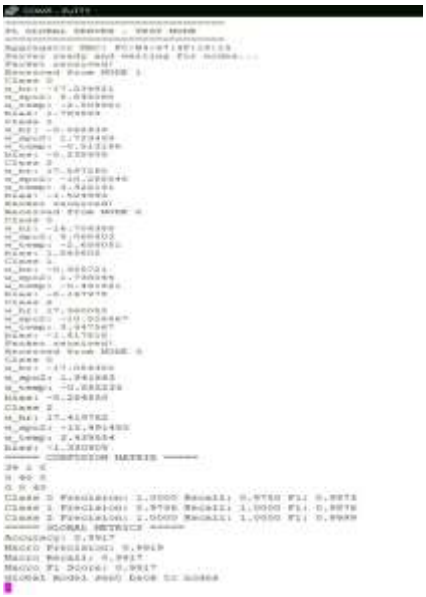

Figure 3: Training results of Federated Learning

4.3 Classification Performance Analysis

The effectiveness of the final worldwide model was assessed with common measurements (Accuracy, Precision, Recall, F1-Score). The Figure 4 implies that the Precision scores were the best for the Critical class, showing that it was very good at spotting high-risk patients. The Recall results were also strong for Critical cases, which is really important in healthcare to make sure that no critical cases are overlooked.

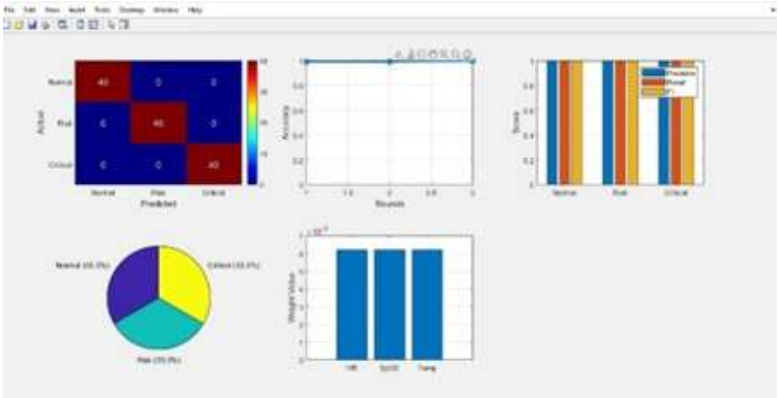

Figure 4: Visualization of performance metrics and confusion matrix

4.4 Communication and Privacy Analysis

The federated method greatly lessened the network strain compared to systems that keep sending unprocessed data all the time. The amount of bandwidth used for each training session was very low because the logistic regression model weights were not heavy. Tests showed that at no point was any unprocessed health data sent to the main server, which naturally decreased the chances of attacks and effectively allowed for private, decentralized health monitoring.

5. CONCLUSION

The testing shows that the new IoT healthcare monitoring system, which uses federated learning, can accurately classify health data while keeping patients' information private. Using a simple SoftMax logistic regression model on limited ESP32 microcontrollers proves that decentralized machine learning can work effectively in real-life situations. The system manages to achieve an impressive mix of 99.17% accuracy, good communication efficiency, the ability to grow, and strong data protection. In the future, improvements will aim to add encryption for sending information and to increase the variety of data for better health understanding.

ACKNOWLEDGEMENT

Our sincere thanks and profound sense of gratitude for the permission provided to utilize the SERB laboratory in the Department of Electronics and Communication Engineering, SRM Valliammai Engineering College, for the completion of the project successfully.

REFERENCES

[1] K. S. Arikumar, A. M. K. Al-Ali, and M. A. Al-Ali, “FL-PMI: Federated Learning-Based Person Movement Identification Through Wearable Devices in Smart Healthcare Systems,” Sensors, vol. 22, no. 3, pp. 1–18, 2022.

[2] S. Baghersalimi, M. H. Kashani, and A. J. Casson, “Personalized Real-Time Federated Learning for Epileptic Seizure Detection,” IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 2153–2164, May 2022.

[3] H. Elayan, M. Aloqaily, and M. Guizani, “Deep Federated Learning for IoT-Based Decentralized Healthcare Systems,” in Proc. IEEE International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 1736–1741.

[4] E. Brophy, Z. Wang, and G. Ward, “Estimation of Continuous Blood Pressure from PPG via a Federated Learning Approach,” Sensors, vol. 21, no. 19, pp. 1–16, 2021.

[5] M.-Y. Chen, “Establishing a Cybersecurity Home Monitoring System for the Elderly Using IoT and Federated Learning,” IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2581–2590, Apr. 2022.

[6] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” in Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[7]J. Konečný, H. B. McMahan, and D. Ramage, “Federated Optimization: Distributed Machine Learning for On-Device Intelligence,” arXiv:1610.02527, 2016.

[8]Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning: Concept and Applications,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, Feb. 2019.

[9]T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, May 2020.

[10]P. Kairouz et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021.

[11]A. Rieke et al., "The Future of Digital Health with Federated Learning," npj Digital Medicine, vol. 3, no. 119, pp. 1–7, 2020.

[12] X. Xu, X. Li, and Y. Zhang, "A Secure and Efficient Federated Learning Framework for IoT-Based Healthcare Applications," IEEE Access, vol. 9, pp. 123456–123468, 2021.

[13]Y. Liu, X. Chen, J. Liu, and C. Zhang, "Secure Federated Learning for IoT-Based Healthcare Systems with Differential Privacy," IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15700–15710, Nov. 2021.

[14]M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A Joint Learning and Communications Framework for Federated Learning Over Wireless Networks," IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 269–283, Jan. 2021.

[15]S. R. Pokhrel and J. Choi, "Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges," IEEE Transactions on Communications, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.