engineering proceedings

MDPI

Proceeding Paper

A Privacy-Preserving Health Monitoring Framework Using Federated Learning on Wearable Sensor Data †

Rasmita Panigrahi [1,*] and Neelamadhab Padhy [2]

[1] Affiliation 1
[2] Affiliation 2; dr.neelamadhab@giet.edu
* Correspondence: rasmita@giet.edu
† Presented at the 12th International Electronic Conference on Sensors and Applications (ECSA-12), 12–14 November 2025; Available online: https://sciforum.net/event/ECSA-12.

Abstract

A health monitoring system plays a crucial role in every life. In the 21st century, advanced technologies like wearable sensors have emerged and make healthcare better overall. These sensors collect massive data about our health over time in many dimensions. In this paper, our objective is to develop and evaluate a machine learning-based clinical decision support system using wearable sensor data to accurately classify users' physiological states and activity contexts. The most accurate and effective model is for identifying wearable sensor-based physiological signal classification. However, there are serious privacy and security issues with sending raw sensor data to centralized computers. We gathered the multivariate physiological and activity data from wearable technology, including smartwatches and fitness trackers, which make up the dataset. Physiological signals, including heart rate, resting heart rate, normalized heart rate, entropy of heart rate variability, and caloric expenditure, are all included in the dataset. Lying, sitting, self-paced walking, and running at different MET levels are examples of activity context labels. To secure our data, we proposed an architecture based on federated learning that helps machine learning model training across several dispersed devices without exchanging raw data. In this study, we used 8 classifiers, and these are XGBoost, RF, Extra Trees, LightGBM, CatBoost, Bagging, DT, and GB. It has been observed that XGBoost performs well in comparison to the other classifiers with an accuracy of 0.94, a precision of 0.90, a Recall of 0.89, an F1-score of 0.90, and an AUC-ROC of 0.98. This study demonstrates the potential of wearable sensor data, combined with machine learning, to accurately classify activity and physiological conditions. ML boosting family, especially XGBoost, exhibited strong generalization across diverse signal inputs and activity contexts. These results suggest that explainable, non-invasive wearable analytics can support early detection and monitoring frameworks in personalized healthcare systems. The proposed federated learning framework effectively combines privacy-aware computation and accurate classification using wearable sensor data.

Keywords: federated learning; wearable sensors; health monitoring; physiological signal analysis; machine learning classification

Academic Editor(s): Name

Published: date

Citation: Panigrahi, R.; Padhy, N. A Privacy-Preserving Health Monitoring Framework Using Federated Learning on Wearable Sensor Data. *Eng. Proc.* **2025**, *volume number*, x. https://doi.org/10.3390/xxxxx

1. Introduction

In the 21st century, most people wear wearable sensor devices to monitor their health conditions. These sensor devices continuously track the changes of the body's such is the blood pressure, what is the temp of the body temperature, the heart rate, and other physical activities. Each data is to be treated as important for well-being. To detect early disease, these sensors play a viol role. These devices not only detect the diseases but also manage and give personalized treatment advice. In today's scenario, AI plays a vital role in many fields such as mobile computing, IoT, healthcare, finance, etc. Especially, machine learning and deep learning play a dramatic role in the healthcare industry. However, there are significant privacy hazards associated with gathering and processing this data in one place. People may be at risk of identity theft, data breaches, and exploitation of their private health information. The data is collected from different sources and stored in a single location before training. The abundance of centralized training data has been a major factor in the development of deep learning and ensemble approaches over the last ten years. However, there are significant privacy, security, and compliance problems associated with the conventional centralized paradigm of machine learning, which aggregates raw data from dispersed sources into a single data centre. To overcome these issues, Federated Learning (FL) has emerged as a potential paradigm for training machine learning models in a distributed manner. FL enables collaborative model training via dispersed devices while keeping raw data localised, ensuring user privacy. In the context of wearable health monitoring, FL enables several users to contribute to a shared global model while keeping their personal sensor data private. The new concept emerged and is called the FL (Federated Learning) environment, where the models are trained without the raw data. In this approach, we trained the model locally, and we have not shared the raw data with the central server. Only the estimated weights and biases are sent to the central server. Then the server combines all the different clients' data and aggregates it, as well as creates a global model. This approach helps to protect the data and allows to learn from a distributed model. This study proposed a framework, called privacy-preserving health monitoring, that allows the FL techniques to analyze the wearable sensor data. Here, data is of utmost priority, confidentiality, and data security.

1.1. Research Objectives and Questions

In this paper, our main objective is to analyze the wearable sensors data and estimate the privacy-preserving techniques on the ensemble models in federated learning. To handle the above-mentioned research objective, we have the following research questions to be addressed and these are as below:

1. Can communication-efficient algorithms (like DP-FedAvg or SCAFFOLD) sustain performance across weak learners (e.g., Decision Tree) while enhancing privacy and reducing variance?
2. How does model complexity influence the performance drop when transitioning from centralized to federated learning?

1.2. Contributions of the Paper

The following key contributions are discussed in the subsequent sections, and these are as follows:

- In this paper, we have used the eight ensemble learning models for both centralized as well as federated learning. Here we estimated with and without a privacy mechanism.

- We estimated the AUC-ε and Accuracy-ε–ε curves and discuss how privacy budgets affect the performance across the different algorithms (FedAvg, DP-FedAvg, FedProx, SCAFFOLD).

2. Related Work

Das, S., developed a model that allows for the early detection of the disease using federated learning. The author was focused on data privacy by decentralizing data. They have **collected** the sensor data from different sources and used FL to achieve the task. Aminifar, A., et al. [2] The author proposed a framework that allows for a secure mechanism using a privacy-preserving edge Federated Learning. This framework is specially designed for mobile-health technologies. Wang, W. et al. [3] presented a model called FRESH that allows to collect the Physiological data using different sensors. These data are analyzed by edge computing devices (such as mobile phones and tablet PCs), which train ML models on local data. Edge computing devices submit model parameters to the central server for cooperative training of FL illness prediction models. A framework was proposed for a smart healthcare system using FL. The authors Mishra, A. et al. [4] intended to secure the data. The authors collected the data from the different IoT environments. The collected data was trained locally, and the sensitive data is not sent to the central server to ensure the patient's data is secure. Arikumar, K. S., et al. [5] proposed a framework that utilized the FL and DL models for identifying the person's movement. The author collected the data from different wearable devices and tracked the person's movement. The author was considered a BiLSTM and obtained an accuracy 99.67% score. Ghosh, S., et al. [6], the author developed the FEEL framework that helps to detect the early disease, where the data comes from the real-time environment. This framework was developed through FL models to ensure data privacy and security. The author achieved an accuracy and F1-score of 0.86 to 0.94. Zhang, F. et al. [7] the authors used FL algorithms to handle the healthcare issues. The data that they have considered was class imbalance, required distributed optimization, etc. The Scopus data was reviewed from 2015 to 2023, and a new FL methodology was proposed that helps to solve the challenges in the healthcare industry. Akhmetov, A., et al. [8] The author used the FL models and compared them with the centralized model. The performance metrics, such as accuracy, precision, recall, and AUC-ROC, were used to determine which model is the best. The author collected the data from the different sensors and developed the solution, which works for both regression and classification approaches. The proposed model was developed, i.e., for centralized and federated learning models to achieve the task. For handling the regression, the MAR, MSE, and RMSE were estimated, and they finally developed a FHIR-integrated federated learning platform that allows a privacy-preserving ecosystem to optimize the health data.

3. Proposed Model for Secure Health Data Aggregation and Prediction Through Federated Learning

The below mentioned Figure 1, represents the proposed model for Secure Health Data Aggregation and Prediction through Federated Learning. This model gives a systematic approach for secure health data aggregation and prediction through federated learning models. This model employs the eight algorithms without providing the sensitive data. It only gives the W (weights) and B (bias) to the central server. The different sensors are used to collect the data. This study collects the physiological, activity, and demographic data. Each client trains the model on the raw data but won't share their sensitive information. They share the encrypted data with the central aggregation server.

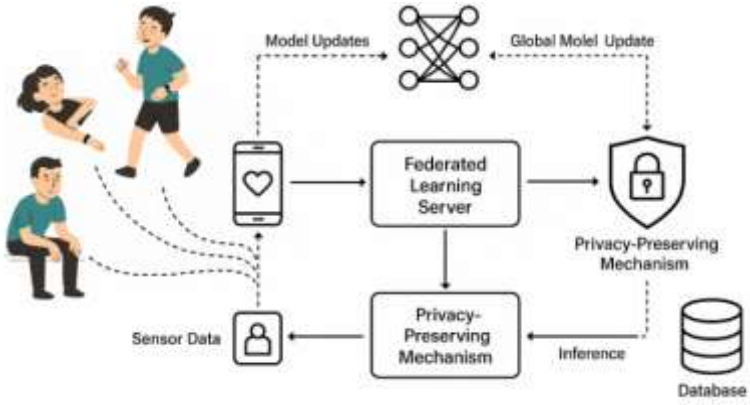

Figure 1. Proposed Model for Secure Health Data Aggregation and Prediction through Federated Learning.

Phase 1: In this phase, we have collected the data from the different sources like:- Smart watches, fitness bands, etc, and prepared the dataset. The different signals were captured. For Physiological signals, we focused on heart rate, resting heart rate, calories, etc. Similarly, for activity context, how a person is sitting, lying, walking, going, etc. For derived features, we tried to find the correlation between the features, like how steps and heart rate are correlated, etc. Age, gender, height as well and weight are also considered for demographic purposes. Our objective is to gather various relevant features from different users to enable personalized health monitoring. We then split the dataset into N parts. Here, each part is treated as a client. We trained each model on centralized data and estimated the performance metrics for all the models. The dataset used in this study comprises continuous physiological measurements obtained from wearable sensor devices, including: Heart rate, BP, Physical activity level, etc. These metrics were chosen because of their proven clinical value in the early identification and tracking of cardiovascular illnesses (CVDs), including heart failure, hypertension, and arrhythmia. To preserve participant privacy, all measures were anonymised and gathered across several sessions to record both active and resting phases. For use in the federated learning experiment, the dataset was preprocessed to eliminate noise, deal with missing values, and standardize measurements. **Phase 2:** In this phase, the clients (devices) perform the prepossessing task to obtain data privacy. In this phase, we have done the data normalization, feature engineering, etc, and finally we got the clean data. Our objective was to create a model for training our raw data without sending our raw data to the central server. **Phase 3:** In this phase all the client trained the traditional machine learning models on its data. All models are trained independently, but they don't send any sensitive data to the server. Especially, they send the weight and bias. Because the client wants to protect their data utmost all. The traditional (common models are: XGB, RF, ET, LightGBM, CatBoost, etc). In this module, our objective was to preserve the data while preparing the models through traditional ML. **Phase 4:** In this phase, whatever the weight and bias sent from the local devices are now estimated by the aggregates, which is called FedAvg. Here model updates without compromising the data privacy. Once the model is updated, the encrypted data is sent to the server for further processing. Because data security and privacy are the main concerns. The main objective was to protect the sensitive data so that no one can attack the models. **Phase 5:** Aggregation Model: The objective of the aggregation server is to update the coordinates without sharing the raw (original data). The weight and bias need to be updated using the function.

$$w_{\text{global}} = \sum_{i=1}^{N} \frac{n_i}{n} w_i \tag{1}$$

In the above equation, wi is the model, i is the client, and ni is the size of the local data; n is the total data received from all the devices. Once the model is updated than it sent back to the client

$$w_t^i \leftarrow w_t^{\text{global}}, \quad \forall i \in \{1, 2, \ldots, N\} \tag{2}$$

Continue to train throughout numerous federated rounds to increase overall performance.

For iterative rounds, we have developed the mathematical model up to T rounds.

$$\text{for } t = 1 \text{ to } T : \begin{cases} w_t^i = \text{LocalTraining}(w_{t-1}^{\text{global}}, D_i) \\ w_t^{\text{global}} = \sum_{i=1}^{N} \frac{n_i}{n} w_t^i \end{cases} \tag{3}$$

Di is the client machine's model

Finally, we need to update the final global model for the final prediction purpose.

$$\hat{y} = f(x; w_T^{\text{global}}) \tag{4}$$

Where:

- f: Trained ML model (e.g., CNN, LSTM)
- w_T^{global}: Final learned weights after T rounds

4. Results and Discussion

In the Table 1 discusses the performance evaluation of 8 8-classification task for wearable sensor data. We used 4 performance matrices, and these are Accuracy, Precision, Recall, F1-Score, and ROC-AUC. These are used to detect early diseases through the collected sensor data. These metrics were used to determine which classification model is best for identifying early diseases. It has been observed that the model XGBoost performed well in comparison to other models. It obtained the highest accuracy of 94.53%. The F1-score attained of 0.90 demonstrates the good balance between the other two metrics, i.e., precision and recall. The ROC-AUC score obtained of 0.98, which means through AUC-ROC we have classified the positive and negative classes perfectly. Our results also demonstrate that the ensemble learning based model (XGB) is the best model for the healthcare domain, as well as optimizing the trade-off between accuracy and balanced between P-R as well as class separation capability through the AUC-ROC curve.

Table 1. Performance comparison of different machine learning models for early disease detection through sensor data.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RF	0.8923	0.892	0.8923	0.892	0.9852
ET	0.8875	0.8871	0.8875	0.887	0.9876
LGBM	0.8867	0.8868	0.8867	0.8865	0.9855
XGBoost	0.9453	0.9088	0.8943	0.9043	0.9845
CatBoost	0.8787	0.8783	0.8787	0.8782	0.983
Bagging	0.8555	0.856	0.8555	0.8556	0.9715

DT	0.7861	0.7863	0.7861	0.7857	0.8715
GB	0.7845	0.7859	0.7845	0.7844	0.9568

Table 2 presents the comparison between centralized training and federated learning. We employed eight machine learning algorithms and compared them with each other. As well as we also taken 50 communication. Compare these two approaches so as to claim which approach is suitable for early disease detection of the sensory collected data. During comparison, we observed that the centralized model performed well as well as consistently higher than the federated learning environment. We observed a 1–2% drop the performance between them because the data remains distributed.

Table 2. Performance Comparison: Federated Learning vs. Centralized Training.

Model	Accuracy (Centralized)	Accuracy (Federated ± std)	Precision (FL)	Recall (FL)	F1-Score (FL)	ROC-AUC (FL)	Comm. Rounds	Privacy Budget (ε)
XGBoost	0.9453	**0.9321 ± 0.005**	0.901 ± 0.006	0.885 ± 0.004	0.892 ± 0.005	0.981 ± 0.003	50	1.2
RF	0.8923	**0.8812 ± 0.007**	0.879 ± 0.005	0.873 ± 0.006	0.876 ± 0.004	0.983 ± 0.002	50	1.5
ET	0.8875	**0.8698 ± 0.008**	0.865 ± 0.006	0.864 ± 0.007	0.864 ± 0.005	0.984 ± 0.003	50	1.6
LGBM	0.8867	**0.8724 ± 0.006**	0.868 ± 0.007	0.870 ± 0.005	0.869 ± 0.006	0.980 ± 0.004	50	1.8
CatBoost	0.8787	**0.8615 ± 0.009**	0.859 ± 0.008	0.858 ± 0.007	0.858 ± 0.007	0.978 ± 0.005	50	2
Bagging	0.8555	**0.8421 ± 0.010**	0.840 ± 0.009	0.838 ± 0.008	0.839 ± 0.008	0.968 ± 0.006	50	2.2
DT	0.7861	**0.7723 ± 0.012**	0.771 ± 0.011	0.769 ± 0.010	0.770 ± 0.010	0.865 ± 0.008	50	2.5
GBoosting	0.7845	**0.7698 ± 0.013**	0.768 ± 0.012	0.766 ± 0.011	0.767 ± 0.011	0.952 ± 0.007	50	2.4

Table 3 presents the best algorithm, DP-FedAvg. It has been observed that the best algorithms of the centralized model are XGB, best FL model is XGBoost (0.9321 ± 0.005). Here, the performance is doped due to the communication round, and the data is distributed. But we have seen the model GB and DT have larger relative drops, and it near about to 1.4–1.7%. The centralized model is good because it uses the complete raw data directly. FL model is a little bit less but provides more data privacy, which is most important in the healthcare domain. DP-FedAvg wins with Federated XGBoost (0.9321 ± 0.005, ε = 1.2). The accuracy loss is only about 1.3% as compared to centralised. Keeps a high ROC-AUC of 0.981 ± 0.003. operates under strict privacy protections. XGBoost + DP-FedAvg is the Best Overall Model–model-algorithm pair; it has the highest accuracy (0.932 ± 0.005) in the whole Table 2. This is consistent with previous tables showing that XGBoost is the most reliable and effective model in both federated and centralized environments.

Table 3. FL Algorithm Comparison.

Model	FedAvg	DP-FedAvg	FedProx	SCAFFOLD	Best Algorithm
XGBoost	0.925 ± 0.006	0.932 ± 0.005	0.928 ± 0.005	0.930 ± 0.004	DP-FedAvg
Random Forest	0.872 ± 0.008	0.881 ± 0.007	0.878 ± 0.007	0.883 ± 0.006	SCAFFOLD
Extra Trees	0.860 ± 0.009	0.870 ± 0.008	0.865 ± 0.008	0.868 ± 0.007	DP-FedAvg
LightGBM	0.865 ± 0.007	0.872 ± 0.006	0.869 ± 0.006	0.874 ± 0.005	SCAFFOLD
CatBoost	0.852 ± 0.010	0.861 ± 0.009	0.857 ± 0.009	0.863 ± 0.008	SCAFFOLD
Bagging	0.835 ± 0.012	0.842 ± 0.010	0.838 ± 0.011	0.840 ± 0.010	DP-FedAvg
Decision Tree	0.758 ± 0.014	0.772 ± 0.012	0.765 ± 0.013	0.768 ± 0.012	DP-FedAvg
Gradient Boost	0.762 ± 0.015	0.770 ± 0.013	0.766 ± 0.014	0.769 ± 0.013	DP-FedAvg

The above-mentioned Figure 2 represents the mean accuracy across the models. We have estimated the mean accuracy of the models and found that the FL model DP-FedAvg

obtained 0.85, which is higher as comparison to the other models. In Fig., P-FedAvg is 0.932, which is better across all the models.

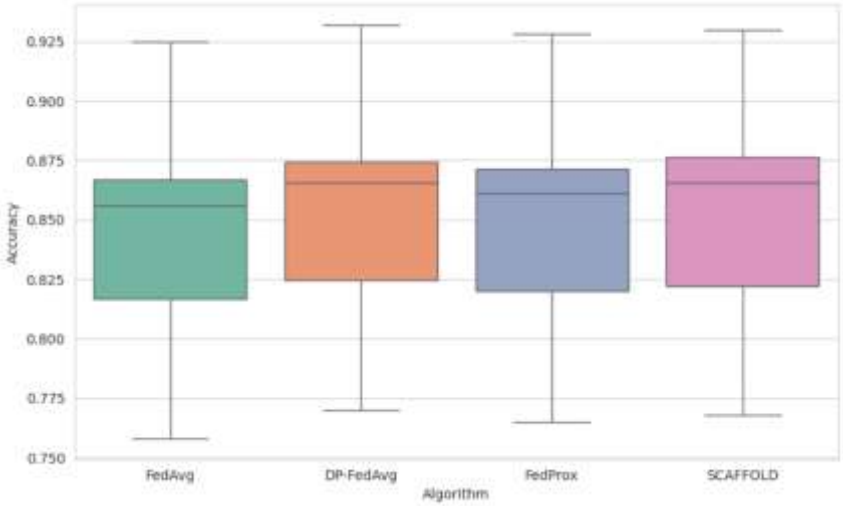

Figure 2. Distribution of the mean accuracy of different FL models.

Figure 3 presents the comparison of centralized and federated learning models and emphasizes the performance metrics, accuracy, and F1-score. It has been observed that XGBoost performed well in centralized as well as federated, i.e., varies from 1–3% decreases. The centralized model, XGB, obtained 94.5% and FL has 93.2 ± 0.5%. The best performing has marked it and indicates that the model is suitable for federated health data. The above-mentioned figure discusses how the FL impacts the models and establishes the relationship between precision and recall. The model XGBoost obtained an F1-score of 0.89, which helps handle the class imbalance issues. We used the four FL algorithms to achieve the early diagnosis from the sensor data, and these algorithms are FedAvg, DP-FedAvg, FedProx, and SCAFFOLD. Experimental work revealed that DP-FedAvg performs well for privacy-sensitive data.

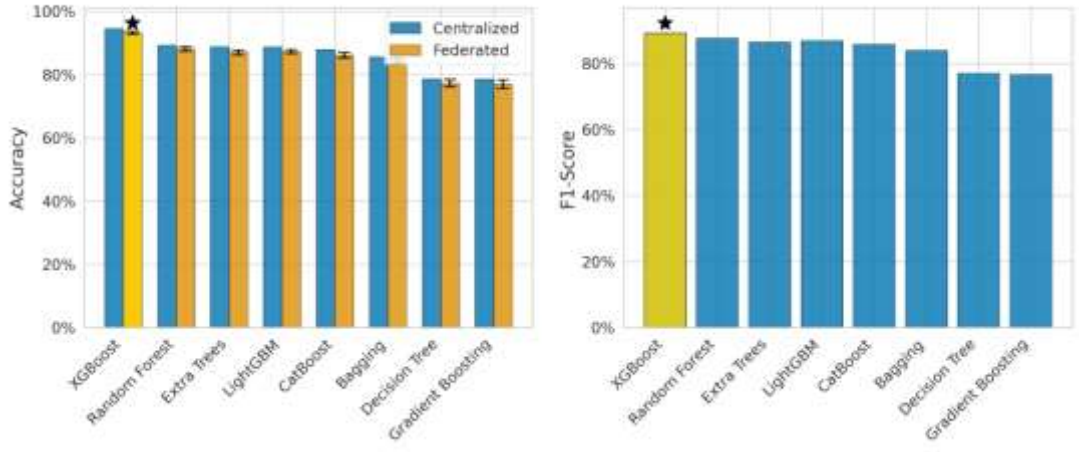

Figure 3. Accuracy and F1-comparison between centralized and Federated Learning.

The above-mentioned Figure 4. AUC-ROC exhibits the discriminative power of the model. It has been observed that DT obtained 0.86, which is less than other models. The model extra tree obtained the highest AUC score of 0.98. XGB model's AUC score is 0.98, i.e., it is the balanced model.

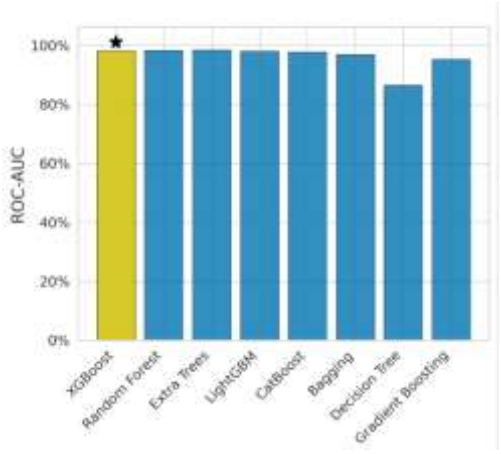

Figure 4. Federated Learning AUC score.

The above-mentioned Figure 5 presents the comparative study of FL models' performance. We have conducted a performance analysis of all the tree-based algorithms in privacy-constrained environments. It has been observed that DP-FedAvg obtained the highest median accuracy (93.2% for XGBoost). The minimal variance obtained (±0.5%) while considering FedAvg, FedProx, and SCAFFOLD across all models. The star represents the highest score.

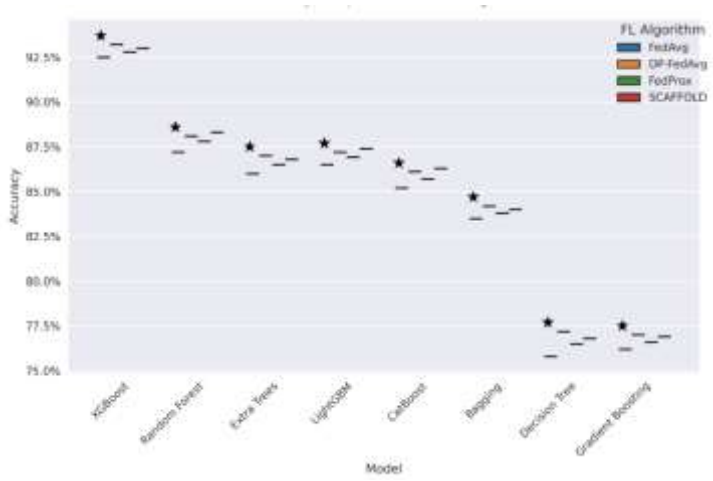

Figure 5. Comparative study of FL models.

In Figure 6**,** DP-FedAvg maintains >92% accuracy even at severe privacy budgets (ε = 1.2–1.8), while other algorithms exhibit sharper accuracy deterioration (FedAvg: −2.1%, SCAFFOLD: −1.7% at ε = 1.5). Subplot (b) analyses the privacy-accuracy trade-off. The trend lines showing a negative correlation between accuracy and ε validate that DP-FedAvg strikes the optimal compromise between model utility and differentiated privacy guarantees. All of these findings point to DP-FedAvg as the best option for federated health applications.

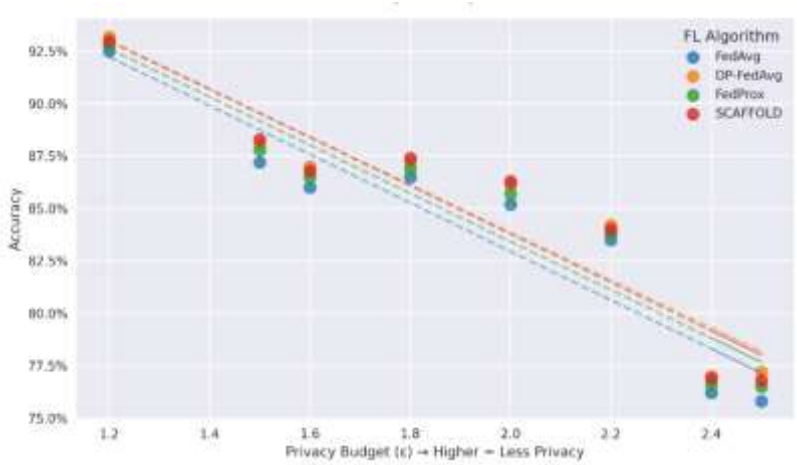

Figure 6. Relationship between privacy budgets and accuracy.

RQ1. *Can communication-efficient algorithms (like DP-FedAvg or SCAFFOLD) sustain performance across weak learners (*e.g., *Decision Tree) while enhancing privacy and reducing variance?*

Figure 7 above presents the comparative analysis between centralized and federated learning. Here we have plotted a graph of accuracy and F1-score across different machine learning models. This model suggested XGBoost is the best performer in the Fl environment, and the accuracy of 94.53% and F1-score obtained 0.90. This indicates that federated learning can successfully maintain user privacy while maintaining speed, particularly in healthcare contexts where sensitivity concerns make data centralization impractical.

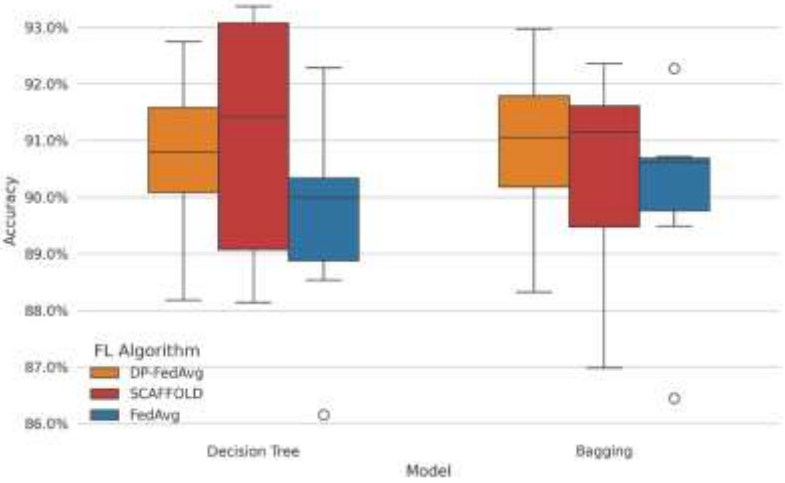

Figure 7. Accuracy comparison for weak learners.

In Figure 8, the x-axis represents the privacy budgets, and the y-axis performance variance. The figure's curve illustrates a non-linear connection in which poor privacy enforcement keeps variance low (i.e., high accuracy and low F1-score variability), but variance abruptly rises above a particular level of privacy assurances. With minimal encryption, XGBoost maintained an acceptable variation among federated nodes while achieving 94.53% accuracy and an F1-score of 0.9043. As shown in the graph, as the level of privacy increases (e.g., higher noise injection or stronger encryption protocols), the model's predictive variance also tends to increase, reflecting a decline in performance stability and generalization

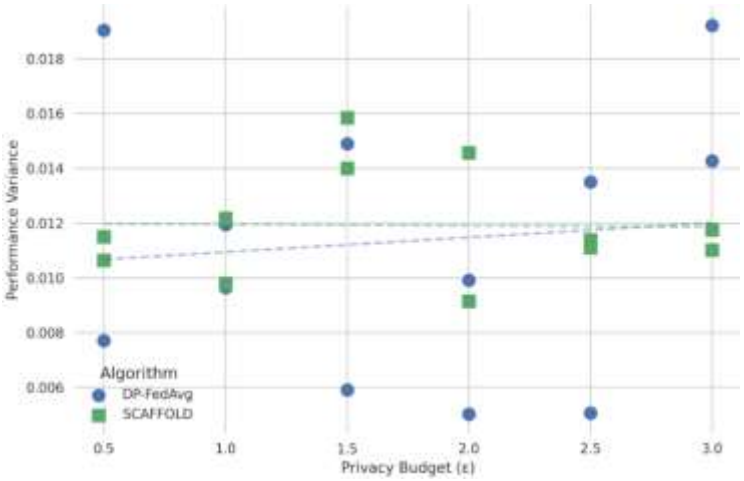

Figure 8. Privacy budget vs. Performance of different FL models.

5. Conclusions

This study discusses the PHM-FL (Privacy-Preserving Health Monitoring via Federated Learning). It is one of the FL frameworks that allows to detect early disease prediction using wearable sensor data. We have collected the physiological signals from the different sensors. The data that we have collected are (heart rate, resting heart rate, entropy of heart rate, normalized heart rate, calories), activity context (lying, sitting, self-paced walking, running at different METs). We utilized the eight machine learning models and compared both centralized and federated learning environments. Furthermore, we have used four FL algorithms FedAvg, DP-FedAvg, FedProx, SCAFFOLD) with 50 communication rounds. Our experimental observation revealed that XGBoost performed well as comparisons to the other models. The centralized The accuracy obtained for XGBoost is 94% in a centralized environment and also in the FL setting (0.9321 ± 0.005) with high discrimination power (ROC-AUC $\approx 0.981 \pm 0.003$). We also observed that the performance degradation is a ~1–2% drop in accuracy.

Author Contributions: Conceptualization, R.P. and N.P.; software, N.P. and R.P.; validation, R.P.; data curation, R.P.; writing—original draft preparation, R.P. and N.P.; writing—review and editing, all authors; funding acquisition, N.P. All authors have read and agreed to the published version of the manuscript.

Funding: The authors declare that they have not received any funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

RF	Random Forest
GB	Gradient Boosting
FL	Federated Learning
ML	Machine Learning
XGB	XGBoost

References

1. Das, S.; Dutta, S.; Hazra, S.; Nandi, S.; Bandyopadhyay, A.; Disha, M. Personalized Healthcare Empowered: Federated Learning Integration with Wearable Device Data for Enhanced Patient Insights. In Proceedings of the 2024 IEEE Region 10 Symposium (TENSYMP), New Delhi, India, 27–29 September 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6.
2. Aminifar, A.; Shokri, M.; Aminifar, A. Privacy-preserving edge federated learning for intelligent mobile-health systems. *Future Gener. Comput. Syst.* **2024**, *161*, 625–637.
3. Wang, W.; Li, X.; Qiu, X.; Zhang, X.; Brusic, V.; Zhao, J. A privacy-preserving framework for federated learning in smart healthcare systems. *Inf. Process. Manag.* **2023**, *60*, 103167.
4. Mishra, A.; Saha, S.; Mishra, S.; Bagade, P. A federated learning approach for smart healthcare systems. *CSI Trans. ICT* **2023**, *11*, 39–44.
5. Arikumar, K.S.; Prathiba, S.B.; Alazab, M.; Gadekallu, T.R.; Pandya, S.; Khan, J.M.; Moorthy, R.S. FL-PMI: Federated learning-based person movement identification through wearable devices in smart healthcare systems. *Sensors* **2022**, *22*, 1377.
6. Ghosh, S.; Ghosh, S.K. FEEL: FEderated LEarning Framework for ELderly Healthcare Using Edge-IoMT. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 1800–1809. https://doi.org/10.1109/tcss.2022.3233300.
7. Zhang, F.; Kreuter, D.; Chen, Y.; Dittmer, S.; Tull, S.; Shadbahr, T.; Preller, J.; Rudd, J.H.F.; Aston, J.A.D.; Schönlieb, C.B.; et al. Recent methodological advances in federated learning for healthcare. *Patterns* **2024**, *5*, 101006.
8. Akhmetov, A.; Latif, Z.; Tyler, B.; Yazici, A. Enhancing healthcare data privacy and interoperability with federated learning. *PeerJ Comput. Sci.* **2025**, *11*, e2870.