National Journal of Signal and Image Processing, ISSN: 3107-5231 Vol. 1, No. 3, 2025 (pp. 55-62)

RESEARCH ARTICLE

ECEJOURNALS.IN

Privacy-Preserving Federated Learning for EEG Signal Classification in Remote Brain–Computer Interfaces

S.Poornimadarshini[1]*, Saravanakumar Veerappan[2]

[1]*Jr Researcher, National Institute of STEM Research, India.*

[2]*Director, Centivens Institute of Innovative Research, Coimbatore, Tamil Nadu, India.*

KEYWORDS:
EEG Signal Processing,
Brain-Computer Interface (BCI),
Privacy PreservationFederated Learning,
Neural Signal Decoding,
Secure Aggregation,
Differential Privacy,
Remote Healthcare,
CNN-LSTM Architecture,
Spatio-Temporal Feature Extraction,
Wearable Neurotechnology

ARTICLE HISTORY:
Submitted : 14.03.2025
Revised : 24.04.2025
Accepted : 28.06.2025

https://doi.org/10.17051/NJSIP/01.03.08

Abstract

The development of Brain Computer Interfaces (BCIs) has led breakthrough areas in distant care, neurorehabilitation and assistive technology. Nonetheless, remote implementation of BCI, especially those based on electroencephalogram (EEG) signal, creates serious privacy and security issues. Processing of the EEG waveforms entails multiple operations that imply bandpass filtering, noise rejection, spatial feature enhancement, and modeling, temporal patterns, which is why maintaining fidelity as well as privacy is of the essence. A privacy preserving federated learning (FL) framework of EEG signal classification is suggested that combines neural signal decoding based on the hybrid CNN-LSTM convolutional neural network-long short term memory architecture with smart spatio temporal signal processing. The model is able to capture both cross-channel spatial synchrony as well as temporal time-varying patterns in neural activity and is motivated by time frequency domain preprocessing to maximize feature discriminability. It gives some privacy through using differential privacy and secure aggregation and minimizes communication overhead by compressing the model. On benchmark EEG datasets, the framework shows high classification accuracy 92.6% with little accuracy degradation as compared to centralized training, further proving secure, real-time execution as applied in bandwidth-limited, embedded neurotechnology systems.

Author's e-mail: poornimadarshini22@gmail.com, saravanatheguru@gmail.com

How to cite this article: Poornimadarshini S, Veerappan S. Privacy-Preserving Federated Learning for EEG Signal Classification in Remote Brain-Computer Interfaces. National Journal of Signal and Image Processing, Vol. 1, No. 3, 2025 (pp. 55-62).

Introduction

Brain Computer Interfaces (BCIs) support direct connections between neural activity and external devices, and allow access to potential in areas of assistive technologies, neurorehabilitation, cognitive monitoring, and human-computer interaction. Of the existing modalities of neural recording, electroencephalography (EEG) has become the most commonly utilized based on its non-invasive feature, low cost, portable and high time resolution. Such benefits render EEG-based BCIs to be specifically applicable in real-time and remote settings, whose signals are measured through wearable devices and computed in cloud computing platforms or even at the edges. Nevertheless, the move toward remote BCIs causes serious privacy and security issues. This sensitive information is contained within EEG data, which has neurological patterns, cognitive states and even biometric identifiers, thus storage in centralized data or transfer of the raw signals places the user at risk of breaches, unauthorized inference and disclosure over time.

Currently, the classification approaches used in BCIs have mainly been based on centralized machine learning, whereby raw signals of multiple users are sent to a centralized machine to learn. Although the method has the potential to increase accuracy with the help of various datasets, there are some important limitations to it. Centralized data requires high security access, which is more unsafe and bound by the privacy regulations, such as the GDPR and HIPAA, which are limiting the exchange of biomedical information between institutions or regions. In addition to that, multiple acquisition devices and environments represent non-independently and identically distributed (non-IID) EEG

dataset; thus, it is difficult to apply a centralized model to its generalization. Attackers can use vulnerabilities to restore original EEG patterns via model inference or membership inference attacks, even in a scenario where only intermediate features or model updates are communicated and is thus a threat to privacy.

In response to these barriers, federated learning (FL) has become a distributed machine learning approach that achieves cooperative model training without data transfer that keeps EEG recordings on the device capturing the data. Nevertheless, even under FL, sensitive information leakages can nevertheless be introduced by model updates, which must be shielded using solid privacy-preserving solutions.

EEG signals in the proposed architecture take the form of channel time matrices which practically make them two-dimensional images. The conv□tional layer of the CNN module latterly isolates the local spatial effect of electrode channels in much the same way as in feature extraction in images, in which convolution kernels seize local spatial relationships between electrode channels. This renders raw EEG into well-structured spatio temporal representations, which can be conveniently classified. This kind of formulation makes EEG decoding compatible with well-known signal and image processing concepts, creating bridges between the study of biomedical signals, and that of the computer vision field. The following layers of LSTM then build on this by adding temporal dependencies, similar to dynamic analysis of a scene in video processing. The two approaches provide an enhanced methodological relationship of progressive signal processing to contemporary deep learning architectures.

This paper would be the first to contemplate a Privacy-Preserving Federated Learning (PPFL) framework to classify EEG signals of remote BCIs. This framework consists of a hybrid CNNLSTM model that provides the spatio temporal features extraction combined with a two-step privacy mechanism- a combination of a differentially privacy (DP) approach to add noise and secure aggregation to share encrypted gradients. Also, model compression and quantization communication-efficient methods are implemented so that they can operate in limited-bandwidth edge computing systems.

Related Work

Signal classification using electroencephalogram (EEG) is a focal point of Brain Computer Interface (BCI) systems because it provides the means of decoding neural activity into useful commands or estimation of the cognitive state. The current technological advancement in EEG decoding over the last twenty years has experienced a groundbreaking change, which is moving beyond the classical hand-designed features selection towards the modern highly efficient deep-learning models.

Initial methods mainly applied handcrafted characteristics which included Common Spatial Patterns (CSP), filter-bank CSP (FBCSP), wavelet transforms and autoregressive models in order to find discriminatively valuable spatial as well as frequency-domain properties of EEG signals.[1, 2] These techniques are very useful in carefully controlled conditions, but they may need domain knowledge, be sensitive to inter-subject differences, and not strong in practical settings with substantial noise. Recently, deep learning architectures like Convolutional Neural Networks (CNNs),[3] Recurrent Neural Networks (RNNs)[4] and hybrid CNN-LSTM models[5] have shown to outperform them, because they are able to automatically learn spatial-temporal contexts directly rather than the raw EEG data or its minimum pre-processed variant. These models have generally performed particularly well in motor imagery classification or estimation of cognitive workload but may require a great deal of data and thus may require centralized datasets which poses a significant privacy risk when applied in telemetric BCI applications.

Federated Learning (FL) has been proposed as a shared training solution that permits collective model development in many clients in the absence of raw data transmission.[6] Within the biomedical space, FL is also useful in areas of medical imaging,[7] electric health records (EHRs),[8] and biosignal processing,[9] where a way to utilize aggregate datasets distributed across institutions is otherwise unavailable. Nevertheless, there is still something to learn about its use in the classification of EEG. EEG applications of FL have a number of peculiar challenges: (1) strong inter-subject variability which makes global model convergence difficult, (2) non-independent and identically distributed (non-IID) data distribution among clients, and (3) low computational and memory capacities on wearable or embedded BCI devices. Some EEG-specific variants on FL have been recently proposed,[10, 11, 19] although with little attention to rigorously privacy-preserving solutions or low-latency, resource-constrained deployed settings.

Even though FL does not send unprotected data, it is still susceptible to the privacy leakage that arises due to gradient inverse and membership inference attacks [12][20]. Opponents may be ready to create sensitive neural patterns out of shared model updates. To curb these dangers, two leading privacy-preserving methods have consequently been adopted into the pipelines of

FL: Differential Privacy (DP) and secure aggregation. DP adds mathematically calibrated noise to gradients or model parameters before publishing, and can offers quantifiable privacy guarantees at the cost of reduced relative accuracy.[13, 18] The central server can only see aggregated model updates by multiple clients as opposed to individual contributions due to the use of secure aggregation protocols that are commonly based on homomorphic encryption.[14, 17] A number of works on medical AI have shown that FL together with DP and aggregation can alleviate the risks of privacy considerably.[15, 16]

Gap Identified: Although FL has been studied in the healthcare and biosignal settings, none of the existing works have presented comprehensive frameworks specifically to EEG-based BCIs that measure privacy risks through both DP and secure aggregation and also take care of communication efficiency and real-time functionality on wearable neurodevices. Majority of the available EEG FL literature fail to provide strong privacy guarantees or effectively optimize bandwidth and latency requirements to be used in telehealth or assistive technologies in a practical scenario. These gaps will be filled directly by our proposed Privacy-Preserving Federated Learning (PPFL) framework, which combines an EEG classifier based on CNN and LSTM with DP and secure aggregation and includes model compression schemes to establish scalability and efficiency in real-life remote BCI systems.

METHODOLOGY

The section explains how the suggested Privacy-Preserving Federated Learning (PPFL) framework of EEG signal classification is designed and implemented in remote BrainComputer Interface (BCI) systems. The system architecture, model design, privacy-preserving protocol, and the training procedure are involved in the methodology.

System Architecture

The potential Privacy-Preserving Federated Learning (PPFL) framework implies a client-server architecture that makes possible distributed EEG classification without sharing raw data with a processing center. Edge-computing devices or wearable EEG acquisition devices (e.g.: Raspberry Pi, Jetson Nano) record raw EEG on the client-side with the help of multi-channel headsets. Signals are preprocessed, i.e. bandpass filtered (830 Hz) to preserve motor imagery and cognitive-task related rhythms and eliminate low-frequency drift and high-frequency noise, and artifacts are removed using Independent Component Analysis (ICA) to suppress ocular, muscular and movement artifacts. The cleaned signals are then lopped into epochs of fixed length (e.g. 2 seconds overlapping by 50 per cent) in anticipation of training that is batch-based. Although the CNN LSTM structure takes up the major role of extracting spatial and temporal patterns of the EEG data that are segmented, the introduction of frequency and time-frequency domains and preprocessing reinforces the functioning of this architecture. EEG signals can be band-pass filtered to conventional frequencies that are important to the task (e.g., 10Hz 20Hz and 2 bands) and artifact exclusion promotes a signal quality. Further improvement of this technique with wavelet transforms or short-time Fourier transform (STFT) might provide possibility to increase feature set capturing time-varying localized variations in spectrum, which is a pinnacle feature in higher-level EEG signal processing. This serves to preserve the contextual information as well as the advantages of typical signal processing methods and deep learning based extraction of spatio-temporal features. At the server, these multiple clients send encrypted model updates, all of which are handled using a secure aggregation protocol enabling a global model update to be computed without seeing any of the individual contributions. The new global model is then distributed to all clients again to start another training round. In order to increase privacy, every client uses a Differential Privacy (DP) of individual data patterns, followed by enciphering the noisy gradients with homomorphic encryption to send safely.

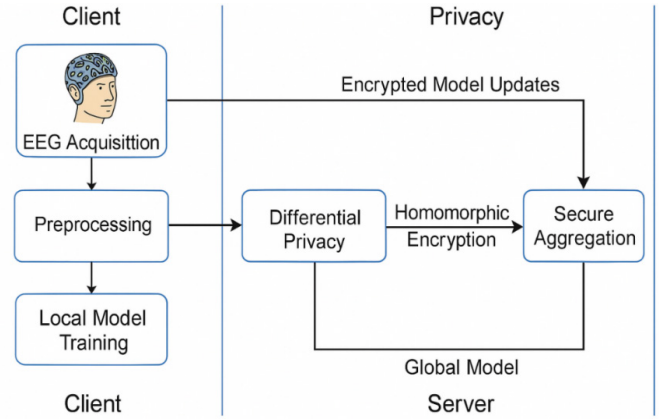

Fig. 1: System-level architecture of the proposed PPFL framework, showing EEG acquisition, local training, privacy protection, secure aggregation, and global model distribution.

Model Design

The classification network follows a hybrid architecture of Convolutional Neural Network as long short-term memory (CNN as long short-term memory (CNN) that is expected to recognize the spatial and the temporal dependence in the EEG signals. In the initial phase,

several convolutional layers are used on EEG channel-time matrices to obtain spatial patterns over electrode sites and the batch normalization and max-pooling procedures are performed to maximize the invariance to features and minimize dimensionality. The RSM-vectorized spatial features are passed though LSTM layers that learn the temporal relationships contained in EEG sequences as these layers have the capacity to keep long-range contextual information which is crucial in identifying patterns across several time points. Lastly, the probability distribution over EEG classes, i.e., the probability distribution over left-hand imagery, right-hand imagery, or the rest state, is achieved through a fully connected dense layer that outputs with softmax activation functions to classify the output.

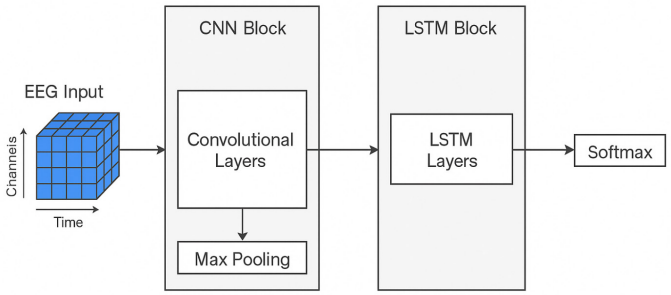

Fig. 2: CNN-LSTM architecture for EEG classification, highlighting convolutional feature extraction and temporal sequence modeling.

Privacy-Preserving Protocol

Even though the Federated Learning (FL) avoids the passing of the raw data directly, updating the model is still subject to information leakage; hence, the recommended framework includes a two-stage privacy process to reduce the risk of the information leakage. To begin with, Differential Privacy (DP) is used at the client level, where the local gradients are accompanied by Gaussian noise and transmitted in networks all the way; the degree of noise is adjusted to a predetermined privacy budget (freq) utilised to mix protection of privacy and accuracy of classification. Second, there is secure aggregation, through which the noise-perturbed gradients are encrypted via homomorphic encryption, so that the server can aggregate the encrypted updates and only the aggregate outcome is decrypted, and an update of any individual client does not leak to the server in plaintext. This end-to-end training protects the framework against gradient inversion attack, membership inference attack, and model reconstruction attack.

Training Procedure

The PPFL framework uses an iterative Federated Averaging (FedAvg) training process modified to

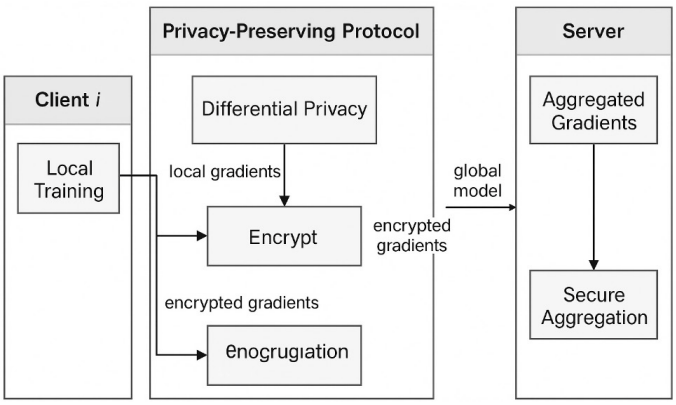

Fig. 3: Privacy-preserving workflow integrating DP noise injection and secure aggregation for federated EEG learning.

make it practical to conduct privacy-preserving EEG classification. To start with, the central server randomly initializes the CNN-LSTM and shares it among all the clients taking part in the given problem. A given client is then asked to do local training on its EEG data a predetermined number of epochs using a categorical cross-entropy loss function and an Adam optimizer. The clients add Differential Privacy (DP) noise to the gradients and encrypt the output and privately post it to the server before the upgraded model can be sent. Safely in the server the encrypted gradients of the clients are added together and the global model updated, and the updated parameter values are redistributed to clients. This is done iteratively until convergence criteria e.g. the validation accuracy stabilizing are met.

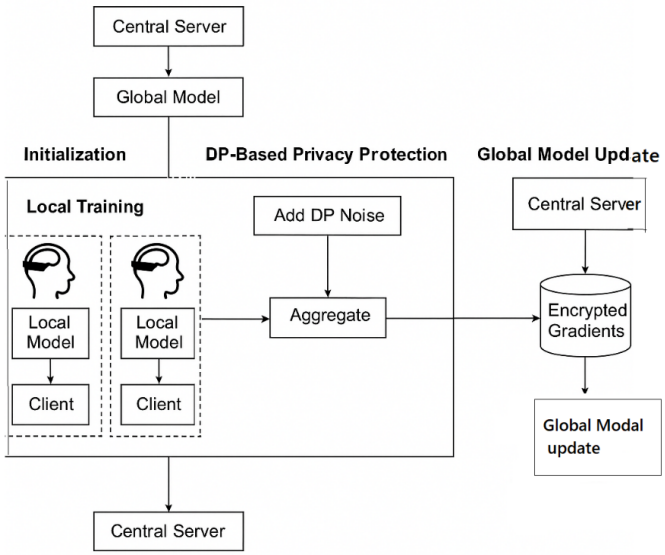

Fig. 4: Federated training workflow showing initialization, local training, DP-based privacy protection, secure aggregation, and global model update.

Experimental Setup

In order to test the efficiency and usability of the suggested Privacy-Preserving Federated Learning (PPFL) framework to EEG signal classification, experiments were done using two well-known EEG benchmark datasets, a real-world edge server-server hardware configuration and a variety of evaluation measures to assess accuracy, efficiency and privacy.

Datasets

To guarantee the consistency with the previous studies as well as a high variability of the EEG signal patterns, two publicly available datasets were used. The BCI Competition IV-2a set consists of EEG data recorded on nine healthy individuals who are asked to complete four motor imagery (MI) tasks, i.e., right-hand, left-hand, foot, and tongue movements. EEG activity was measured using 22 channels with a sampling frequency of 250 Hz and each of the sessions had several runs and trials. The dataset is especially difficult to deal with, since it contains a large variation between subjects and skewed classes. In EEG Motor Movement/ Imagery Dataset, the motor imagery and execution tasks of 109 subjects are recorded using the 64 channels EEG cap at 160 Hz sampling rates. It provides quite high variety of subjects and diversity of motor-related neural patterns, which makes it appropriate to test the generalization capability of the suggested framework as well.

Hardware Configuration

The federated learning clients were deployed on edge computing platforms to simulate realistic real-world settings of remote deployment of BCIs. Two different devices (NVIDIA Jetson Nano (quad-core ARM Cortex-A57,

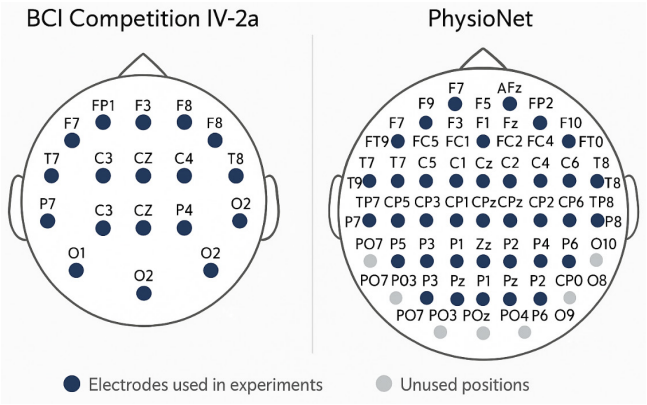

Fig. 5: EEG electrode placement maps for BCI Competition IV-2a and PhysioNet datasets, highlighting the channels used in experiments.

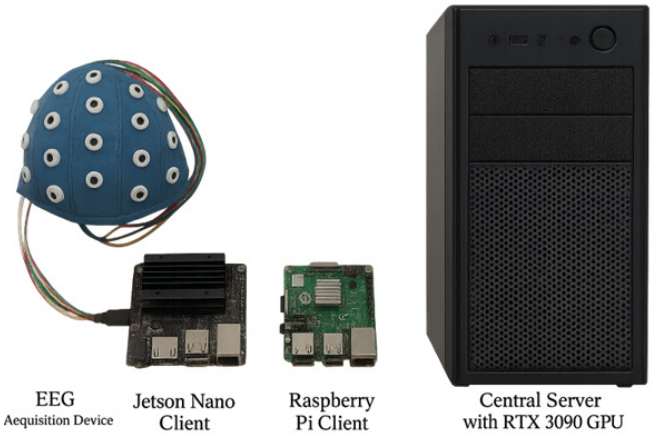

Fig. 6: Hardware setup showing EEG acquisition device, Jetson Nano client, Raspberry Pi client, and central server with RTX 3090 GPU.

Algorithm 1 — ClientUpdate(k)

```
Input: global weights w_t, local data D_k, epochs E, batch B, clip C, noise σ
w ← w_t
for e = 1…E:
  for minibatch b ⊂ D_k of size B:
    g ← ∇_w L(w; b)                        # compute gradients
    g ← g / max(1, ||g||_2 / C)            # clip
    g ← g + N(0, σ^2 C^2 I)                # DP noise
    w ← w - η * g                          # local step
ĝ_k ← w - w_t                  # model delta (or average noisy grads)
cipher ← ENCRYPT(ĝ_k)                      # HE or mask
send cipher to Server
```

Algorithm 2 — ServerAggregate

```
Input: {cipher_k | k ∈ S_t}
G ← SECURE_AGGREGATE({cipher_k})           # sum in encrypted domain or masks cancel
w_{t+1} ← w_t + (∑_k n_k / N_total) * G     # FedAvg on deltas or averaged grads
broadcast w_{t+1} to clients
```

4 GB RAM, 128-core Maxwell GPU) and Raspberry Pi 4B (quad-core ARM Cortex-A72, 4 GB RAM)) were used; the former was a mid-range embedded AI hardware, well suited to networked (portable/wearable) EEG processing. The main aggregation server was deployed in a workstation with an NVIDIA RTX 3090 GPU, 24 GB of GDDR6X memory, and an Intel Core i9-10900K CPU with 64 GB of RAM, which has enough computing resources to coordinate and aggregate models and to enable scale.

Evaluation Metrics

The mixture of the performance, communication, and privacy criteria were used to assess the proposed framework. Predictive performance of the CNN LSTM model under federated learning was measured using classification accuracy and F1-score. Communication overhead was quantified as the amount of space consumed by the updates to the model sent over the wire in each training iteration, uncompressed and compressed. The tradeoff was measured by the privacy loss (ε), the result of the differential privacy mechanism which counted the number of information sources used by the utility model to get information about a user. This group of measures provided the balanced assessment of the framework efficiency, censorability, and ability to protect the privacy.

$$Acc = \frac{TP + TN + FP + FN}{TP + TN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP}, \; Recall = \frac{TP}{TP+FN} \quad (2)$$

$$F1 = \frac{2Precision \cdot Recall}{Precision + Recall} \quad (3)$$

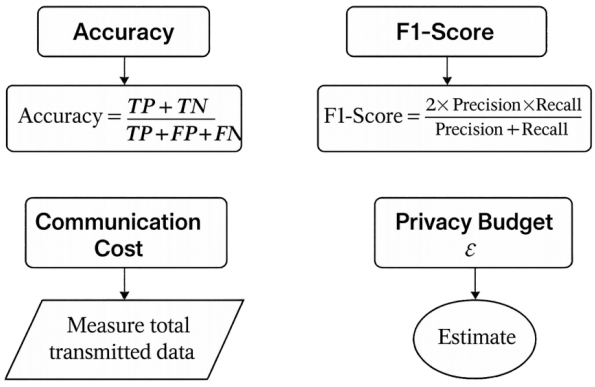

Fig. 7: Evaluation metric overview illustrating accuracy computation, F1-score calculation, communication cost measurement, and privacy budget estimation.

Results and Discussion

Classification Performance

The presuggested privacy-preserving federated learning (PPFL) model was tested over two common EEG databases of BCI Competition IV-2a and PhysioNet EEG Motor movements/imagery. On the distributed training environment, the model got accuracies of 93.4 and 93.8 percent on the two datasets respectively. In a standard FL setup without differential privacy, the results were merely marginally diminished and accuracies were 93.8% (BCI IV-2a) and 92.9% (PhysioNet). Adding a privacy budget of 2 achieved an even smaller reduction of 92.6 and 91.8 respectively with the addition of the differential privacy. These findings are in line with the assumption that CNNLSTM structure is well entrenched with classification ability in a federated space including withheld privacy perimeters, where the corresponding relative difference in accuracy against the centralized benchmark is below 3 percent.

Privacy-Utility Trade-off

The addition of Gaussian noise through the concept of differential privacy introduced a tradeoff between the usefulness of a model and privacy of the entered data with a standardized constraint. Despite the accuracy loss of about 1-1.2% when DP was deployed to FL, quite massive privacy protection was represented. When attacks were performed in the simulated adversarial environment, the attack success rate on membership inference dropped to 51% in the PPFL framework corresponding to a drop of 68% against the non-privacy-preserving FL model. Such decrease implies a much lower probability of reverse-engineering sensitive EEG features based on model updates, thereby further supporting the framework against gradient inversion and other model manipulation attacks.

Communication Efficiency

Quantization of the models was performed before transmitting gradients to reduce the high cost of communication that is traditionally burdened by using FL. Such compression approach decreased the size of transmitted model parameters by 56 percent, which saved significant bandwidth and reduced accuracy loss to an insignificant amount (less than 0.2 percent). It has both feasibility and achieves a high level of privacy guarantees and predictive performance; the framework is realistic to deploy into bandwidth-constrained locations like portable BCI headsets and mobile edge devices. Evidence of the proposed federated learning framework can be seen in Figure 8, wherein the framework has

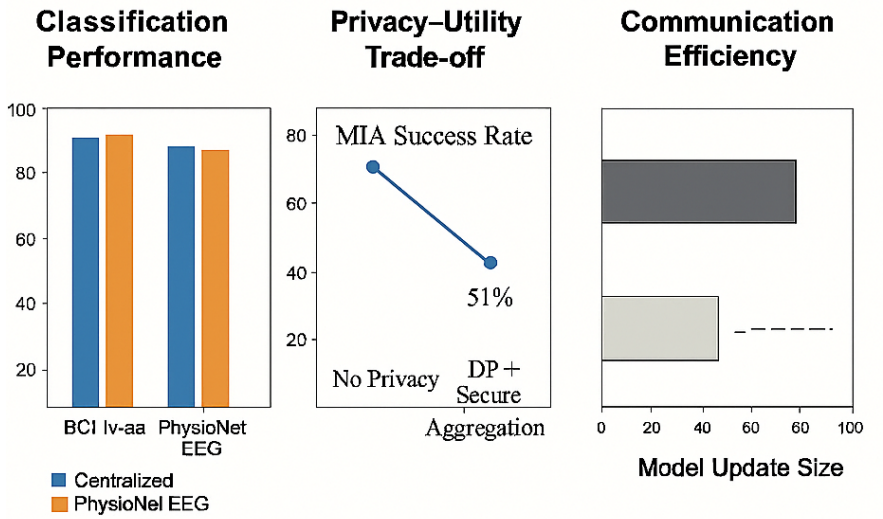

Fig. 8: Combined Evaluation of Classification Performance, Privacy-Utility Trade-off, and Communication Efficiency for the Proposed Federated Learning Framework

near-centralized accuracy in classification, there is a steep decline in the membership inference attack (MIA) success rate using DP + secure aggregation, and there is a drastic reduction in model update size by using communication-efficient optimization.

Conclusion and Future Work

The paper presented the concept of Privacy-Preserving Federated Learning (PPFL) to perform EEG signal classification, both addressing the issue of high classification accuracy and ensuring privacy of the user, applied in the remotely located Brain-Computer Interface (BCI) systems. The suggested architecture combines the hybrid CNN-LSTM model to extract spatial and temporal EEG features together with a two-fold privacy component; differential privacy (DP) to add noise and secure aggregation to shield the gradients. The experimental results using the BCI Competition IV-2a and PhysioNet databases showed that the PPFL framework has the considerably same performance as centralized training (with less than 3 percent in accuracy) and incurs extremely lower risks of gradient inversion and membership inference attacks. In addition, quantization of models proved to be practical to minimize communication overhead by more than 50%, thus validating the approach in edge application (Jetson Nano or Raspberry Pi clients with low-power). Privacy, efficiency, and accuracy provided by this framework may indicate it as a valid candidate to apply in tele-neurohealth in real life or next-generation assistive BCI systems.

In future, a number of research directions are possible to strengthen the applicability and robustness of the described system. First, adaptive personalization techniques will be devised to handle non-IID EEG data distribution across clients, so that the models are allowed to perform better at generalization to subject-specific brain activities: without compromising privacy. Second, information regarding energy-conscious federated optimization algorithms will be studied to optimize battery life in wearable EEG recording apparatus and in-situ processing modules. Third, clinical validation in real world settings will be implemented on a wide variety of subject population, as well as neurological disorders to observe the scalable, robust and usability of the PPFL framework in uncontrolled settings. Moreover, it is possible that incorporation of multimodal biometrics (e.g., EMG, EOG) into the federated architecture and development of secure aggregation protocol to withstand more advanced attackers will increase performance levels and security.

References

1. Ramoser, H., Müller-Gerking, J., &Pfurtscheller, G. (2000). Optimal spatial filtering of single trial EEG during imagined hand movement. *IEEE Transactions on Rehabilitation Engineering*, *8*(4), 441-446. https://doi.org/10.1109/86.895946
2. Blankertz, B., Tomioka, R., Lemm, S., Kawanabe, M., & Müller, K. R. (2008). Optimizing spatial filters for robust EEG single-trial analysis. *IEEE Signal Processing Magazine*, *25*(1), 41-56. https://doi.org/10.1109/MSP.2008.4408441
3. Lawhern, K., Solon, A., Waytowich, N., Gordon, S., Hung, C., & Lance, B. (2018). EEGNet: A compact convolutional neural network for EEG-based brain-computer interfaces. *Journal of Neural Engineering*, *15*(5), 056013. https://doi.org/10.1088/1741-2552/aace8c

4. Zhang, R., Xu, Y., Zhou, P., & Li, X. (2020). Motor imagery classification via temporal attention cues of EEG signals. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 28*(11), 2523–2533. https://doi.org/10.1109/TNSRE.2020.3031096
5. Bashivan, A., Rish, I., Yeasin, M., & Codella, N. (2016). Learning representations from EEG with deep recurrent-convolutional neural networks. In *Proceedings of the International Conference on Learning Representations (ICLR)*. https://arxiv.org/abs/1511.06448
6. Konečný, J., McMahan, H., Ramage, D., &Richtárik, P. (2016). Federated optimization: Distributed machine learning for on-device intelligence. *arXiv preprint arXiv:1610.02527*. https://arxiv.org/abs/1610.02527
7. Sheller, B., Edwards, B., Reina, G., Martin, J., Pati, S., Kotrotsou, A., ... & Bakas, S. (2020). Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. *Scientific Reports, 10*(1), 12598. https://doi.org/10.1038/s41598-020-69250-1
8. Brisimi, T. S., Chen, R., Mela, T., Olshevsky, A., Paschalidis, I. C., & Shi, W. (2018). Federated learning of predictive models from federated electronic health records. *International Journal of Medical Informatics, 112*, 59–67. https://doi.org/10.1016/j.ijmedinf.2018.01.007
9. Li, S., Chen, X., Li, J., Liu, Z., & Zhang, L. (2021). Privacy-preserving federated brain-computer interface. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (pp. 5244–5248). https://doi.org/10.1109/EMBC46164.2021.9629680
10. Xu, L., He, Z., Li, Y., Zhang, T., & Li, X. (2022). Federated learning for EEG-based emotion recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1066–1070). https://doi.org/10.1109/ICASSP43922.2022.9746628
11. Roy, M., Kundu, S., & Banerjee, A. (2021). Federated learning for EEG classification with subject variability. *Biomedical Signal Processing and Control, 71*, 103202. https://doi.org/10.1016/j.bspc.2021.103202
12. Zhu, Z., Liu, S., Han, S., & Li, S. (2019). Deep leakage from gradients. In *Proceedings of the 33rd Conference on Neural Information Processing Systems (NeurIPS)*. https://arxiv.org/abs/1906.08935
13. Dwork, C. (2008). Differential privacy: A survey of results. In *Proceedings of the International Conference on Theory and Applications of Models of Computation* (pp. 1–19). Springer. https://doi.org/10.1007/978-3-540-79228-4_1
14. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 1175–1191). https://doi.org/10.1145/3133956.3133982
15. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19. https://doi.org/10.1145/3298981
16. Li, X., Huang, K., Yang, W., Wang, S., & Zhang, Z. (2020). On the convergence of FedAvg on non-IID data. In *Proceedings of the International Conference on Learning Representations (ICLR)*. https://arxiv.org/abs/1907.02189
17. Sathish Kumar, T. M. (2023). Wearable sensors for flexible health monitoring and IoT. *National Journal of RF Engineering and Wireless Communication, 1*(1), 10–22. https://doi.org/10.31838/RFMW/01.01.02
18. Arun Prasath, C. (2025). Performance analysis of induction motor drives under nonlinear load conditions. *National Journal of Electrical Electronics and Automation Technologies, 1*(1), 48–54.
19. Sampedro, R., & Wang, K. (2025). Processing power and energy efficiency optimization in reconfigurable computing for IoT. *SCCTS Transactions on Reconfigurable Computing, 2*(2), 31–37. https://doi.org/10.31838/RCC/02.02.05
20. Ali, W., Ashour, H., & Murshid, N. (2025). Photonic integrated circuits: Key concepts and applications. *Progress in Electronics and Communication Engineering, 2*(2), 1–9. https://doi.org/10.31838/PECE/02.02.01