1. Bouchiba GUELTA [1], 2. Samir BENBAKRETI[2], 3. Kadda BOUMEDIENE[3]

University of Science and Technology of Oran USTO-MB (1, 3), Higher National School of Information and Communication Technologies and Post (2)

doi:10.15199/48.2024.06.07

Differentially Private federated learning to Protect Identity in Stress Recognition

Abstract. *Over the last decade, the use of Automatic emotion recognition has become increasingly widespread in response to the growing need to improve human life quality. The used emotion data encompasses a wealth of personal information, which includes but is not limited to gender, age, health condition, identity, and so on. These demographic information, known as soft or hard biometrics, are private and the user may not share them with others. Unfortunately, with the adversarial algorithms, this information can be inferred automatically, creating the potential for user's data breach. To address the above issues, we present a federated learning–based approach to hide identity-related information in identity subject task, while maintaining their effectiveness for emotion utility task. We also introduce differential privacy mechanism, a method that explicitly limits the data leakage from federated learning model. Experiments conducted on the WESAD dataset demonstrate that stress recognition tasks can be effectively carried out while decreasing user identity and ensuring differential privacy guarantees; the intensity of the amount of noise derived from differential privacy can be tuned to balance the trade-off between privacy and utility.*

Streszczenie. ciągu ostatniej dekady zastosowanie automatycznego rozpoznawania emocji stało się coraz bardziej powszechne w odpowiedzi na rosnącą *potrzebę poprawy jakości życia człowieka. Wykorzystywane dane dotyczące emocji obejmują bogactwo danych osobowych, które obejmują między innymi płeć, wiek, stan zdrowia, tożsamość itd. Te informacje demograficzne, zwane miękkimi lub twardymi danymi biometrycznymi, są prywatne i użytkownik nie może udostępniać ich innym osobom. Niestety, w przypadku algorytmów kontradyktoryjnych informacje te mogą zostać wywnioskowane automatycznie, co stwarza ryzyko naruszenia bezpieczeństwa danych użytkownika. Aby rozwiązać powyższe problemy, przedstawiamy stowarzyszone podejście oparte na uczeniu się, mające na celu ukrycie informacji związanych z tożsamością w zadaniu podmiotu tożsamości, przy jednoczesnym zachowaniu ich skuteczności w zadaniu użyteczności emocjonalnej. Wprowadzamy także mechanizm różnicowej prywatności, metodę, która wyraźnie ogranicza wyciek danych z federacyjnego modelu uczenia się. Eksperymenty przeprowadzone na zbiorze danych WESAD pokazują, że zadania rozpoznawania stresu można skutecznie wykonywać, zmniejszając jednocześnie tożsamość użytkownika i zapewniając zróżnicowane gwarancje prywatności; intensywność hałasu pochodzącego z różnicowej prywatności można dostroić, aby zrównoważyć kompromis między prywatnością a użytecznością.* (***Różnorodnie prywatne stowarzyszone uczenie się w celu ochrony tożsamości w rozpoznawaniu stresu***)

Keywords: Stress recognition, Federated learning, Differential privacy, Deep learning
Słowa kluczowe: Rozpoznawanie stresu, Uczenie stowarzyszone, Prywatność różnicowa, Uczenie głębokie

Introduction

The growing demand for wearable devices and the widespread adoption of the Internet of Things (IoT) in real-world applications have paved the way for ubiquitous personal health tracking [1]. In affective recognition application, IoT devices collect electronic data on emotional states using a variety of sensors and transmit this emotional data to an application server for processing and analysis. Notably, the service provider employs advanced machine learning techniques to determine the represented human state levels, including valence and arousal dimensions [2]. While the cloud server offers valuable benefits, it raises a critical concern regarding the potential access, whether intentional or accidental, to sensitive user information [3]. Indeed, data breaches, compromised servers or any unwanted exploitation of the data expose users to personal and sensitive information leakage such as health-related attributes [4]. Advancements in perturbation and cryptographic techniques offer potential solutions for safeguarding user data against privacy concerns [5]. Nonetheless, the intricate data protection process requires more time, making it impractical for real-time applications and relies on substantial computational resources like GPUs [6].

Federated learning has recently shown its strong ability for privacy preserving in several domains because of the ability to allow clients to train their own data on their local machines without the need to share them with a cloud server [7]. Despite enhancing privacy by limiting the exposure of personal data, Federated Learning (FL) remains susceptible to various threats; for example, it is not resilient against model poisoning which aims to disrupt the convergence of the central model [8, 9]. Privacy breaches can also occur through membership inference attacks, where the presence of an individual data record in the training data inferred, or through attribute inference attacks, where adversaries can deduce sensitive information about individuals [9]. The adversary has the potential to manipulate the training model and intercept communication between the server and the client [8-9]. To address these concerns, diverse strategies have been suggested, including the adoption of Differential Privacy at both of local user or server level, along with the utilization of lightweight cryptographic and differential privacy methods [10].

Motivated by the latter researches, we propose to combine the federated learning approach and differential privacy scheme to balance between the utility and privacy trade-off. We evaluate the proposed noise injection method over both tasks using WESAD [11] dataset. We show that the proposed approach can effectively maintain the important features for the stress recognition task while perturbing the features contributing to reveal human identity task.

Related works

The recognition of stress levels through physiological sensors has gained significant attention in recent years. Thanks to the availability of advanced sensors capable of gathering multi-modal physiological data for emotion recognition [12]. To the best of our knowledge, a few studies using FL have been done to solve numerous practical privacy issues in this area, most of them focused on speech-emotion recognition [13, 14, 15].

In the speech and audio domain, FL has mainly been used for emotion recognition while preserving the demographic information of the users. For instance, Latif et al. [16] explored a Federated Learning (FL) approach for emotion recognition tasks, where only the model was shared among clients. They utilized an LSTM classifier and conducted experiments on the EMOCAP dataset, which encompassed four emotions: happiness, sadness, anger and neutrality.

Tsouvalas et al. [15] employed a semi-supervised approach based on CNN for federated learning to learn and predict emotion labels from the device speaker. Nevertheless, this method does not guarantee the privacy of the data. This primary concern is confirmed by Feng et al. [13], which proposed a scenario of attack against the shared model in the decentralized learning framework for Speech Emotion Recognition (SER).

Zhao, Huan et al. [17] integrated a BiLSTM model with a self-attention mechanism into the Federated Learning (FL) framework. This was done to mitigate automatically sensitive demographic characteristics while preserving the performance utility for a specified emotion in utterances during Speech Emotion Recognition (SER) training.

Chao, et al. [18], proposed a gender privacy protection method called Gender-Indistinguishability (GenderInd) and conducted experiments using different privacy protection methods to defend against attacks.

Ali, Hafiz Shehbaz et al. [19] used an auto encoder to transform the original space into latent space, which combined with a decoder to reconstruct only feature emotion categories and with multi-classifier-based gradient reversal (GRL) to unlearn sensitive information gender, identity speaker and language classification. To evaluate the proposed model, authors validated and tested their approach on fourth databases, IEMO-CAP, EMODB, EMOVO and BUEMODB.

In the case of using physiological based modality, Gahlan, Neha et al. [20] used Federated Learning (FL) model for predicting perceived stress based on physiological data. Each sub-client employed an MLP classifier to train its local data on the edge and shared individual updated parameters of the MLP using the FedAVG algorithm.

Nandi, Arijit et al. [21], introduced Fed-ReMECS, a machine-learning model for emotion recognition built upon an FL framework. To discern valence and arousal levels, they employed wavelet feature extraction along with a neural network, utilizing Electro dermal Activity (EDA) and respiration data from the DEAP dataset. Their approach is subsequently validated.

Anwar, Mohd Ayaan et al. [22] conducted research on classifying emotion states from EEG physiological signals while ensuring the privacy of users' data. They employed a federated learning approach based on neural networks to extract more discerning features from EEG signals sourced from the DREAMER dataset.

Chhikara, Prateek, et al. [23] integrated both face and speech modalities using the Federated Learning (FL) approach. In the case of the face modality, they utilized a combination of CNN and SVM models, while for the audio modality, they applied a 2D CNN model to process extracted spectrogram images, the proposed framework underwent validation and testing on two distinct datasets: FER2013 for facial emotion recognition and Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS) for speech emotion recognition. Inspired by the aforementioned
works, we designed stress recognition system under the private FL combined with differential privacy settings to show that adding an amount of noise derived from DP in a federated setting can help balance the utility and privacy trade-off.

Proposed framework

This section provides a detailed description of the proposed framework. As illustrated in Fig. 1, we initially pre-process and extract a set of meaningful features from the raw multi-physiological signals. Subsequently, we introduce a federated learning module to train the extracted feature data using deep learning models, which are designed for stress recognition. Additionally, we explore the impact of adding noise to the updated federated learning model to reduce information leakage from the gradient model.

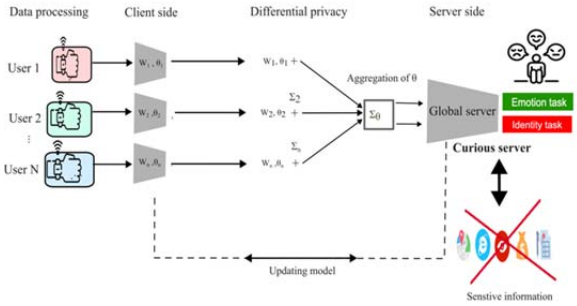

Fig. 1 Architecture of our proposed framework

Data description

To validate the proposed approach, we adopted the WESAD dataset [11] released for affective state monitoring. Each participant recorded a range of physiological signals including blood volume pulse, electrocardiogram, electro dermal activity, electromyogram, respiration, body temperature and three-axis acceleration (see Fig. 2). These were measured from the chest and wrist using RespiBAN and Empatica E4 devices. Fifteen individuals (12 males and three females) took part in the study, which encompassed four states: baseline, amusement, stress and meditation. Additional details can be found in [11].

Table 1. Lists of feature extraction methods applied on WESAD dataset

Modality type	Feature	Description
ECG	BRM HRV HRV(RMS)	Beats per minute Heart rate variability Root mean squared of HRV
Resp	RESPindur RESPexdur RESPrate	Inspiration duration Expiration duration Respiration rate
EDA	SCL(Mean) SCL(Std) SCL(Var)	Average skin conductance level Standard deviation of SCL Variance of SCL
ACC	ACC(Mean) ACC(Var) ACC(RMS) ACC(FFT) ACC(Ske) ACC(Kur) ACC(En)	Mean Variance root mean square FFT energy, Skewness Kurtosis Entropy

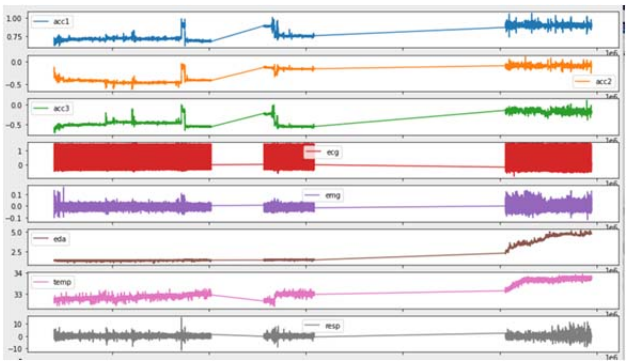

Fig. 2 Multi physiological signals visualization WESAD

Only five modalities have been used in our work: electrocardiogram (ECG), electro-dermal activity (EDA), respiration (Resp) and three-axis acceleration (ACC). Each physiological signal is segmented into windows of 700 samples with a 20% overlap, resulting in a total of 185,814 segments. To maximize the correlation among inter-subjects and minimize among subjects, these segments were further processed for extracting an important feature being extracted from temporal and frequency domains as explained in table 1.

Federated learning approach

The federated learning (FL) paradigm, in contrast to conventional training methods, involves training models directly on user devices. This approach allows users to keep their data localized on their own devices and exchange locally updated models for specific learning tasks with a central server.

The main objective of this algorithm is to iteratively train a learning model M under the supervision of the server by aggregating locally trained models from each participant. In each communication round i, every client k fine-tunes its local model using its own data, implementing Stochastic Gradient Descent (SGD) across several local and global communication rounds. In the synchronous version, after participants transmit their model updates to the server, the server preforms averaging scheme over these updates using and transmitted back to to all devices.

(1) $$M_{i+1=\sum_{k=1}^{K}\frac{n_c}{n}m_k^{k+1}}$$

With n_c the set of indexes of all the data points n on client k, $m_k^{i+1}$the local update of a client k, calculated with the following equation:

(2) $$m_c^{i+1} = m_c^i - \eta g_c^i$$

With η a fixed learning rate (i.e., hyperparameter which controls the step size of the optimization) for each client and g_c^i the average gradient on the local data of the client k at the epoch i. Those learning rounds continue until the convergence of the central model.

In traditional Federated Learning (FL), the global model is computed by averaging over the models of client participants, a method that suitable in homogeneous FL environments. However, this shared model may contain sensitive and private information, such as gender, age, or biometric user templates, making it vulnerable to inference or adversarial attacks [24]. This requires the use of a perturbation method to limit the potential leakage of the black box gradient exchanged model [25]. To address this concern, we have adopted Differential Privacy (DP) schemes to safeguard either local or global data during FL model training. This method implies to inject the noise before uploading the local Stochastic Gradient Descent (SGD) model to the global server using a synthetic noise derived from specific distribution such as Gaussian or Laplace [24]. A formal definition of differential privacy is defined by this following:

A set of noise distributions can be sampled from the DP mechanism (DP). A randomized mechanism D on the training set with domain $\mathfrak{D}$ and range R satisfies DP (ε, δ) for two small positive numbers and if the following inequality holds [10]:

(3) $$Pr(\mathcal{M}(D) \in S) \leq e^{\varepsilon}\, Pr(\mathcal{M}(D') \in S) + \delta$$

Where D and $D' \in \mathfrak{D}$ are two input neighbour datasets, and $S \subseteq R$ (i.e., R is set of all possible outputs), δ is privacy loss or failure probability and ε is privacy budget. In simple terms, DP mechanism takes two input neighbour datasets and applies a perturbation function where the likelihood ratio between two distributions is bounded by e^{ε}. This process can be represented by Fig. 3.

An optimal Differential Privacy (DP) mechanism aims for a reduced δ value and a smaller ε value. However, these adjustments often lead to a decrease in function utility, as measured by metrics like accuracy. Therefore, the crucial consideration is determining the extent to which we should perturb DP values while maintaining a satisfactory balance between privacy and utility. The DP perturbation is defined as sensitivity function expressed as:

(4) $$\Delta f = max\|M(D) - M(D')\|_1$$

And scaling noise can be computed as:

(5) $$\sigma = \Delta f/\varepsilon$$

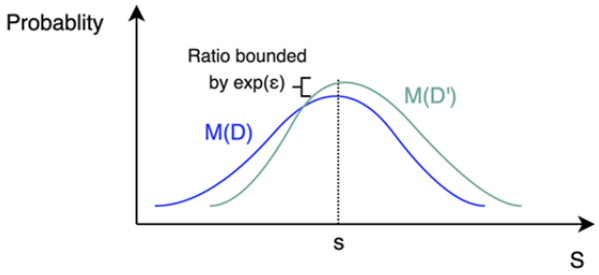

Fig. 3 Example of Differential privacy

In this study, for compliance with (ε, δ)-Differential Privacy standards, it is essential to appropriately scale the Laplace and Gaussian distributions. For instance, the Gaussian DP mechanism is defined as:

(6) $$M_{i+1=\sum_{k=1}^{K}\frac{n_c}{n}m_k^{k+1}} + \mathcal{N}(0, \sigma^2 C^2 I)$$

Where N: probabilistic distribution function, C: clipping threshold.

Experimental Results:

To assess the effectiveness of the proposed framework, we created three scenarios: centralized, federated averaging learning FedAvg and FedAvg with differential privacy. Their performances are evaluated on the WESAD dataset, which consists of multi- modal physiological signals collected from 15 individuals.

The utility task aims to recognize the users' emotion (i.e., stress vs no stress). The privacy task is referred to the people identity identification task, in which the adversary attempts to identify the people belong to this dataset.

For classification module, we used four classifiers namely: probabilistic neural network (PNN), one-dimensional convolutional neural network (1D-CNN), gated recurrent unit (GRU) and recurrent, neural network (RNN).

PNN is trained using SGD consisting of a single hidden layer with 28 hidden units, where fine-tuning of this model is only the spread parameter sigma (δ_{pnn} =0.2) to prevent vanishing gradient network. The output network represents the number of class for each task.

CNN is trained using SGD consisting of 3 convolutional layers with the convolutional kernel size 5 and the padding size 4, where ReLU units and softmax of 15 classes are applied. For time series model classification, every single classifier (LSTM, RNN, GRU) consists of 70 memory cells, a dropout layer and followed by full activation layer. We use

the cross-entropy loss function and SDG Learning rate (β=0.0005) for all models.

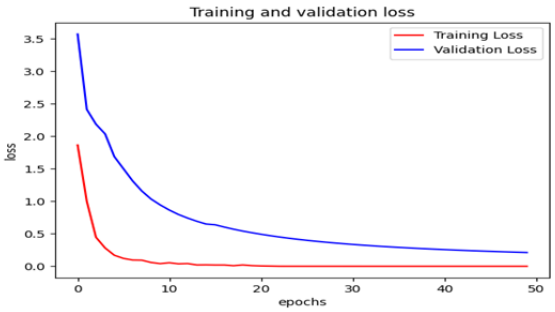

Fig. 4 Training and validation loss curve (1D CNN model)

The accuracy metric and confusion matrix are used to assess the performance of the proposed framework. In each simulation scenario, we run 10-fold cross-validation, where each fold is tested based on the training of the other. For instance, Fig. 4 shows the training and validation loss obtained from 1DCNN model.

Centralized learning (CL) approach:

We carry out the CL approach on the WESAD data set as a baseline experiment. Here, only server training model is considered to train and test the whole dataset. We set the maximum number of training epochs to 50. Table 1 shows the accuracy results obtained from all classifiers. We can see the performance of both tasks, stress and identity recognition are quite similar.

The higher results has been achieved by the 1DCNN model. Fig. 5 and 6 show the confusion matrix of our centralized learning approach.

The results confirm the potential information leakage in this case, which maintains model accuracy while revealing user identity. As a result, this learning approach could not prevent the user from data breach attacks.

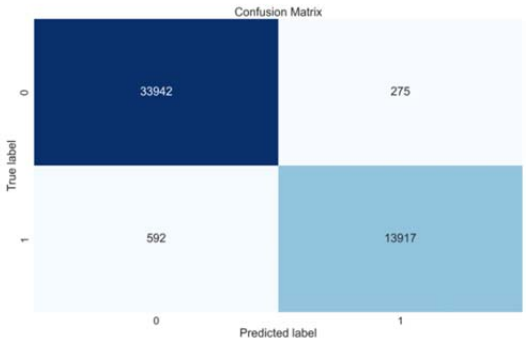

Fig. 5. Confusion Matrices of 1D CNN model on the WESAD dataset (Stress recognition based centralized learning approach)

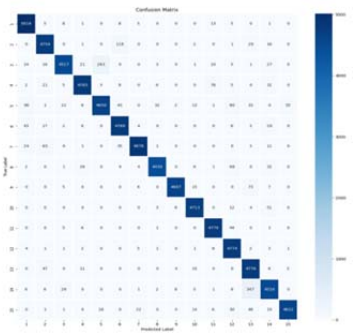

Fig 6. Confusion Matrices of 1D CNN model on the WESAD dataset (Identity recognition based centralized learning approach)

Table 2. Performance of stress recognition (AUC) using centralized learning approach

	PNN	1DCNN	LSTM	GRU	RNN
Utility task	0.82	0.98	0.93	0.93	0.89
Privacy task	0.78	0.96	0.90	0.91	0.82

Vanilla federated learning approach

In the second experiment, we evaluate the performance of federated learning on the stress recognition task. We set a number of clients (K=5, 10, 20) and each client holds Di instance from the whole dataset. To limit the information leakage from local model, we set the number of epoch to 5 and the number of communication round between the clients and server is 50.

Form table 3, the best performance result achieved with 1DCNN classifier, where the stress recognition achieves 95% and identity recognition 82%. The matrix confusion also confirmed these results. (See Fig. 8 and 9).

As we expected, increasing the client participation during the training FL model, it leads to improve the performance model.

We also studied the effect of data distribution, independent and non-independent identically distributed (IID vs No-IID). In IID, we consider instance's labels are distributed equally, where the No-IID are not disturbed equally. From Fig. 8, we can observe that No-IID affects the performance model.

Since the FL privacy guarantee often relies on the server, SGD training might reveal sensitive information about the client using adversarial attack or model inversion attacks [25].

Table 3. Performance of stress recognition (AUC) using vanilla federated learning approach

	PNN	1DCNN	LSTM	GRU	RNN
Utility task	0.75	0.95	0.89	0.90	0.80
Privacy task	0.65	0.82	0.75	0.78	0.72

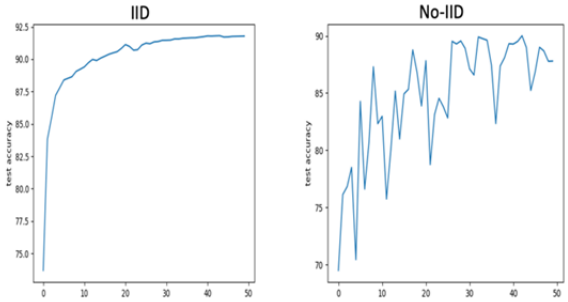

Fig 7. Impact of the data distribution on the FL performance (Stress recognition task (IID vs No-IID))

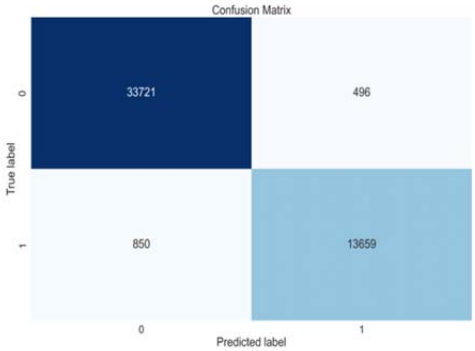

Fig. 8. Confusion Matrices of 1D CNN model on the WESAD dataset (Stress recognition based vanilla federated learning approach)

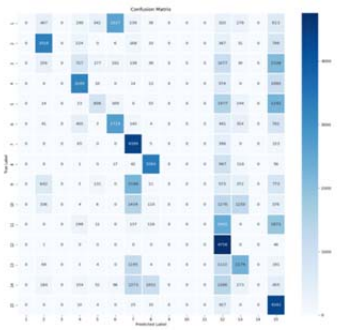

Fig. 9. Confusion Matrices of 1D CNN model on the WESAD dataset (Identity recognition based vanilla federated learning approach)

Federated learning with differential privacy:

To maintain the privacy, we incorporated the differential privacy in the federated learning model. As we explained in the previous section, we scaled the noise injected to the local training model from DP- based Gaussian mechanism perturbation [24]. To study the effect of noise amount, it should be injected to balance between the utility and privacy trade-off, the selected DP values are ε=3, ε=10, ε=15, ε= 30 and ε=80 where δ fixed to 0.001.

(7) $$\sigma = \sqrt{\frac{2log\frac{1.25}{\delta}}{\varepsilon}}$$

As comparison with vanilla FL, we used the same FL parameters of pervious experiment.

From Table 4, results show that FL with DP mechanism provides better performance while decreasing the identity recognition task. The results confirmed in the confusion matrix (see Fig. 10 and 11).

We also investigate the impact of DP parameters on the proposed framework's performance. From Table 5, the obtained results show that increasing the amount of noise in the local training model decreases the implementation of the privacy task. However, it also leads to worse utility task performance.

Increasing the DP budget values and communication rounds of the local training model negatively affects the trade-off between utility and privacy tasks. It improves identity recognition performance.

Table 4. Performance of stress recognition (AUC) using FL learning with DP (epsilon=10) approach

	PNN	1DCNN	LSTM	GRU	RNN
Utility task	0.60	0.90	0.76	0.80	0.70
Privacy task	0.45	0.65	0.55	0.63	0.52

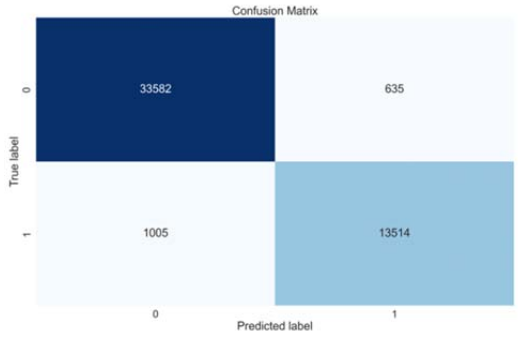

Fig 10. Confusion Matrices of 1D CNN model on the WESAD dataset (Stress recognition based federated learning with DP approach)

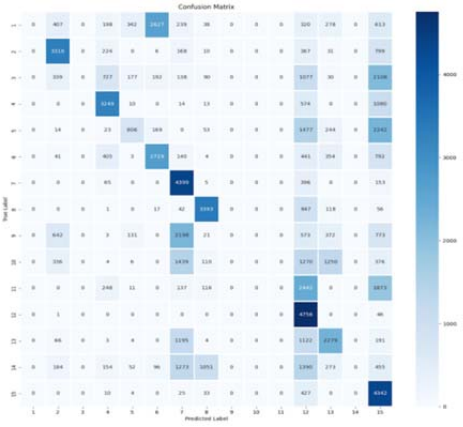

Fig 11. Confusion Matrices of 1D CNN model on the WESAD dataset (Stress recognition based federated learning with DP approach)

Table 5. Impact of the DP budget level on FL performance

DP budget	Ep=3	EP=10	EP=15	EP=30	EP=80
Utility task	0.65	0.90	0.92	0.92	0.94
Privacy task	0.35	0.65	0.78	0.80	0.82

Conclusion

In this work, we investigated the effectiveness of federated learning in practical recognition studies. These results show that federated learning enables the users to perform their utility tasks without exposing their data to the central server. It provides a better utility and privacy trade-off than an FL vanilla approach by incorporating differential privacy in the locally trained model before sharing it with the global server. Among our essential observations, we discovered that the distribution of labels across clients can decrease the model performance. Motivated by this fact, we plan to investigate how we can improve FL-based stress recognition within heterogeneous settings.

Conflicts of Interest)

The authors declare no conflict of interest.

REFERENCE

[1] Mohr, David C., Mi Zhang, and Stephen M. Schueller. "Personal sensing: understanding mental health using ubiquitous sensors and machine learning." Annual review of clinical psychology 13 (2017): 23-47.

[2] Zeng, Zhihong, et al. "A survey of affect recognition methods: audio, visual and spontaneous expressions." Proceedings of the 9th international conference on Multimodal interfaces. 2007.

[3] Kairouz, Peter, et al. "Advances and open problems in federated learning." Foundations and Trends® in Machine Learning 14.1–2 (2021): 1-210.

[4] Ibbett, Alan. "An examination of real-world data leakage from IoT devices." (2022).

[5] Turgay, Safiye, and İlker İlter. "Perturbation Methods for Protecting Data Privacy: A Review of Techniques and Applications." Automation and Machine Learning 4.2 (2023): 31-4.

[6] Roman, Adrian-Silviu. "Evaluating the Privacy and Utility of Time-Series Data Perturbation Algorithms." *Mathematics* 11.5 (2023): 1260.

[7] Zhang, Chen, et al. "A survey on federated learning." *Knowledge-Based Systems* 216 (2021): 106775.

[8] Lyu, Lingjuan, Han Yu, and Qiang Yang. "Threats to federated learning: A survey." *arXiv preprint arXiv:2003.02133* (2020).

[9] Shao, Jiawei, et al. "A Survey of What to Share in Federated Learning: Perspectives on Model Utility, Privacy Leakage, and Communication
Efficiency." arXivpreprintarXiv:2307.10655 (202)

[10] El Ouadrhiri, Ahmed, and Ahmed Abdelhadi. "Differential privacy for deep and federated learning: A survey." *IEEE access* 10 (2022): 22359-22380.
[11] Philip Schmidt, A., R. Duerichen Reiss, and Introducing WESAD Kristof Van Laerhoven. "a multimodal dataset for wearable Stress and Affect Detection." *Proceedings of the International Conference on Multimodal Interaction*. 2018.
[12] Zhang, Jianhua, et al. "Emotion recognition using multi-modal data and machine learning techniques: A tutorial and review." *Information Fusion* 59 (2020): 103-126.
[13] Feng, Tiantian, et al. "Attribute inference attack of speech emotion recognition in federated learning settings." *arXiv preprint arXiv:2112.13416* (2021).
[14] Zhang, Tuo, et al. "Fedaudio: A federated learning benchmark for audio tasks." *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2023.
[15] Tsouvalas, Vasileios, Tanir Ozcelebi, and Nirvana Meratnia. "Privacy-preserving speech emotion recognition through semi-supervised federated learning." *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 2022.
[16] Latif, Siddique, et al. "Federated learning for speech emotion recognition applications." *2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2020
[17] Zhao, Huan, et al. "Privacy-Enhanced Federated Learning Against Attribute Inference Attack for Speech Emotion Recognition." *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 202. an,
[18] Chao, et al. "General or Specific? Investigating Effective Privacy Protection in Federated Learning for Speech Emotion Recognition." ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 202.
[19] Ali, Hafiz Shehbaz, et al. "Privacy enhanced speech emotion communication using deep learning aided edge computing." *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021.
[20] Gahlan, Neha, and Divyashikha Sethia. "Federated learning inspired privacy sensitive emotion recognition based on multi-modal physiological sensors." *Cluster Computing* (2023): 1-23.
[21] Nandi, Arijit, and Fatos Xhafa. "A federated learning method for real-time emotion state classification from multi-modal streaming." *Methods* 204 (2022): 340-347.
[22] Anwar, Mohd Ayaan, et al. "FedEmo: A Privacy-Preserving Framework for Emotion Recognition using EEG Physiological Data." *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2023.
[23] Chhikara, Prateek, et al. "Federated learning meets human emotions: A decentralized framework for human–computer interaction for IoT applications." *IEEE Internet of Things* Journal 8.8 (2020): 6949-6962.
[24] Abadi, Martin, et al. "Deep learning with differential privacy." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.
[25] Geiping, Jonas, et al. "Inverting gradients-how easy is it to break privacy in federated learning?." *Advances in Neural Information Processing Systems* 33 (2020): 16937-16947.